



“十二五”职业教育国家规划教材

网络设备安装与调试 (锐捷版)

余运祥 陆 沁 汪双顶 主 编



电子工业出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书根据教育部颁发的《中等职业学校专业教学标准（试行）信息技术类（第一辑）》中的相关教学内容和要求编写而成。本书的编写从满足经济发展对高素质劳动者和技能型人才的需求出发，在课程结构、教学内容、教学方法等方面进行了新的探索与改革创新，利于学生更好地掌握本课程的内容，利于学生理论知识的掌握和实际操作技能的提高。

本书以实际工作应用场景为背景，介绍了日常企业网组建、安装过程中涉及的交换机上架，交换机、路由器、无线局域网设备及网络安全产品的配置、安装和调试技术。学生在组建局域网的过程中，能学会设备选型，能根据设备的性能和技术参数选择合适的组网设备。

本书由8个项目组成，涉及局域网组建过程中，使用到重要的组网设备及应用在设备上的关键技术等，如配置交换机设备、虚拟局域网技术、生成树技术、链路聚合技术、干道技术、静态路由技术、动态路由技术、地址转换技术、广域网接入安全认证技术、交换机端口安全、访问控制列表技术、防火墙技术、无线局域网技术等，通过全部或部分技术的学习，基本上掌握局域网组建过程中常用的设备的安装、配置和调试技术，训练未来工作中需要掌握的技术和技能。

本书可作为计算机网络技术的专业核心课程教材，也可作为各类计算机网络培训班的教材，还可以供中小型企业网建设与管理人员参考学习。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

网络设备安装与调试：锐捷版 / 余运祥、陆沁、汪双顶主编. —北京：电子工业出版社，2018.8

ISBN 978-7-121-24909-9

网... 余... 朱... 计算机网络—通信设备—设备安装—中等专业学校—教材
TN915.05

中国版本图书馆 CIP 数据核字（2014）第 275010 号

策划编辑：关雅莉

责任编辑：裴 杰

印 刷：

装 订：

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本：787×1 092 1/16 印张：12 字数：307.2 千字

版 次：2018 年 8 月第 1 版

印 次：2018 年 8 月第 1 次印刷

定 价：35.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010) 88254888，88258888。

质量投诉请发邮件至 zltts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：(010) 88254617，luomn@phei.com.cn。

编审委员会名单

主任委员：

武马群

副主任委员：

王 健 韩立凡 何文生

委 员：

丁文慧	丁爱萍	于志博	马广月	马永芳	马玥桓	王 帅	王 苒	王晓姝
王家青	王 彬	王皓轩	王新萍	方 伟	方松林	孔祥华	龙天才	龙凯明
卢华东	由相宁	史完美	史晓云	冯理明	冯雪燕	毕建伟	朱文娟	朱海波
向 华	刘小华	刘天真	刘 凌	刘 猛	关 莹	江永春	许昭霞	孙宏仪
苏日太夫	杜宏志	杜秋磊	杜 珺	李 飞	李华平	李宇鹏	李 娜	杨 杰
杨 怡	杨春红	吴 伦	何 琳	余运祥	邹贵财	沈大林	宋 微	张士忠
张文库	张 平	张东义	张兴华	张呈江	张 侨	张建文	张 玲	张凌杰
张媛媛	陆 沁	陈丁君	陈天翔	陈观诚	陈佳玉	陈泓吉	陈学平	陈 玲
陈道斌	陈 颜	范铭慧	罗 丹	周海峰	周 鹤	庞 震	赵艳莉	赵晨阳
赵增敏	郝俊华	胡 尹	钟 勤	段 欣	段 标	姜全生	钱 峰	徐 宁
徐 兵	高 强	高 静	郭立红	郭 荔	郭朝勇	黄汉军	黄 彦	黄洪杰
崔长华	崔建成	梁 姗	彭仲昆	葛艳玲	董新春	韩雪涛	韩新洲	曾平驿
曾祥民	温 晞	谢世森	赖福生	谭建伟	戴建耘	魏茂林		

序 | PROLOGUE

当今是一个信息技术主宰的时代，以计算机应用为核心的信息技术已经渗透到人类活动的各个领域，彻底改变着人类传统的生产、工作、学习、交往、生活和思维方式。和语言与数学等能力一样，信息技术应用能力也已成为人们必须掌握的、最为重要的基本能力。职业教育作为国民教育体系和人力资源开发的重要组成部分，信息技术应用能力和计算机相关专业领域专项应用能力的培养，始终是职业教育培养多样化人才、传承技术技能、促进就业创业的重要载体和主要内容。

信息技术的发展，特别是数字媒体、互联网、移动通信等技术的普及应用，使信息技术的应用形态和领域都发生了重大的变化。第一，计算机技术的使用扩展至前所未有的程度，桌面电脑和移动终端（智能手机、平板电脑等）的普及，网络和移动通信技术的发展，使信息的获取、呈现与处理无处不在，人类社会生产、生活的诸多领域已无法脱离信息技术的支持而独立进行；第二，信息媒体处理的数字化衍生出新的信息技术应用领域，如数字影像、计算机平面设计、计算机动漫游戏、虚拟现实等；第三，信息技术与其他业务的应用有机地结合，如与商业、金融、交通、物流、加工制造、工业设计、广告传媒、影视娱乐等结合，形成了一些独立的生态体系，综合信息处理、数据分析、智能控制、媒体创意、网络传播等日益成为当前信息技术的主要应用领域，并诞生了云计算、物联网、大数据、3D 打印等指引未来信息技术应用的发展方向。

信息技术的不断推陈出新及应用领域的综合化和普及化，直接影响着技术、技能型人才的培养定位，并引领着职业教育领域信息技术或计算机相关专业与课程改革、配套教材的建设，使之不断推陈出新、与时俱进。

2009 年，教育部颁布了《中等职业学校计算机应用基础大纲》；2014 年，教育部在 2010 年新修订的专业目录基础上，相继颁布了计算机应用、数字媒体技术应用、计算机平面设计、计算机动漫与游戏制作、计算机网络技术、网站建设与管理、软件与信息服务、客户信息服务、计算机速录等 9 个信息技术类相关专业的教学标准，确定了教学实施及核心课程内容的指导意见。本套教材就是以此为依据，结合当前最新的信息技术发展趋势和企业应用案例组织开发和编写的。



本套系列教材的主要特色

● 对计算机专业类相关课程的教学内容进行重新整合

本套教材面向学生的基础应用能力，设定了系统操作、文档编辑、网络使用、数据分析、媒体处理、信息交互、外设与移动设备应用、系统维护维修、综合业务运用等内容；针对专业应用能力，根据专业和职业能力方向的不同，结合企业的具体应用业务规划了教材内容。

● 以岗位工作过程来确定学习任务和目标，综合提升学生的专业能力、过程能力和职位差异能力

本套教材通过工作过程为导向的教学模式和模块化的知识能力整合结构，体现产业需求与专业设置、职业标准与课程内容、生产过程与教学过程、职业资格证书与学历证书、终身学习与职业教育的“五对接”。从学习目标到内容的设计，本套教材不再仅仅是专业理论内容的复制，而是经由职业岗位实践—工作过程与岗位能力分析—技能知识学习应用内化的学习实训引导和案例。借助知识的重组与技能的强化，达到企业岗位情境和教学内容要求相贯通的课程融合目标。

● 以项目教学和任务案例实训作为主线

本套教材通过项目教学，构建了工作业务的完整流程和岗位能力需求体系。项目的确定应遵循三个基本目标：核心能力的熟练程度，技术更新与延伸的再学习能力，不同业务情境应用的适应性。教材借助以校企合作为基础的实训任务，以应用能力为核心，以案例为线索，通过设立情境、任务解析、引导示范、基础练习、难点解析与知识延伸、能力提升训练和总结评价等环节引领学习者在任务的完成过程中积累技能、学习知识，并迁移到不同业务情境的任务解决过程中，使学习者在未来可以从容面对不同应用场景的工作岗位。

当前，全国职业教育领域都在深入贯彻全国工作会议精神，学习领会中央领导对职业教育的重要批示，全力加快推进现代职业教育。国务院出台的《加快发展现代职业教育的决定》明确提出要“形成适应发展需求、产教深度融合、中职高职衔接、职业教育与普通教育相互沟通，体现终身教育理念，具有中国特色、世界水平的现代职业教育体系”。现代职业教育体系的建立将带来人才培养模式、教育教学方式和办学体制机制的巨大变革，这无疑给职业院校信息技术应用人才培养提出了新的目标。计算机类相关专业的教学必须要适应改革，始终把握技术发展和技术技能人才培养的最新动向，坚持产教融合、校企合作、工学结合、知行合一，为培养出更多适应产业升级转型和经济发展的高素质职业人才做出更大贡献！

前言 | PREFACE

为建立健全教育质量保障体系，提高职业教育质量，教育部于 2014 年颁布了《中等职业学校专业教学标准》（以下简称《专业教学标准》）。《专业教学标准》是指导和管理中等职业学校教学工作的主要依据，是保证教育教学质量和人才培养规格的纲领性教学文件。在“教育部办公厅关于公布首批《中等职业学校专业教学标准（试行）》目录的通知”（教职成厅[2014]11 号文）中，强调“专业教学标准是开展专业教学的基本文件，是明确培养目标和规格、组织实施教学、规范教学管理、加强专业建设、开发教材和学习资源的基本依据，是评估教育教学质量的主要标尺，同时也是社会用人单位选用中等职业学校毕业生的重要参考。”计算机网络技术专业的职业范围见下表。

1. 本书特色

本书根据教育部颁发的《中等职业学校专业教学标准（试行）信息技术类（第一辑）》中的相关教学内容和要求编写而成。

为了将产学结合、校企合作的模式真正引入学校的教学改革工作之中，本课程开发小组联合行业知名技术专家与相关职业院校的一线骨干教师教学团队，合作开发了本套工学结合网络互连设备的安装和调试教材。与其他网络类网络互连设备的安装和调试教材不同，本书从一个全新的角度，深入、全面、细致地介绍了交换机、路由器和防火墙的原理、参数、分类、适用范围、规划、接口、连接、配置、管理、监控、故障等诸多方面的内容，涵盖了从网络搭建、设备配置，到网络安全防范、故障诊断的所有重要设备配置技术，是专门为中小型网络管理员量身打造的网络互连设备的安装和调试教程，以迅速完成从学生向专业网管员的过渡。

本书以真实的网络工程项目为背景，基于任务驱动、项目导向的“工学结合”教学模式编写而成。网络互连设备的安装和调试任务都来源于企业工程实践，为便于教学进行了适当调整，使项目具有典型性、实用性和综合性。全书涵盖了初、中级路由、交换及安全设备的全部内容，读者能够通过本项目的实施，完成网络设备安装与调试相关知识的学习与技能训练。

本书可作为计算机网络专业的核心课程教材，也可作为各类计算机网络培训班的教材，还可以供中小型企业网建设与管理人员参考学习。

2. 课时分配

本书各项的教学内容和课时分配建议如下。

项目	课程内容	知识讲解	操作实践	合计
1	配置交换机设备	8	8	16
2	配置路由器设备	8	10	18
3	配置三层交换机设备	6	6	12

续表

项目	课程内容	知识讲解	操作实践	合计
4	配置高级路由技术	6	6	12
5	配置路由器接入广域网	4	6	10
6	配置网络安全技术	6	8	14
7	配置防火墙设备	4	4	8
8	配置无线局域网设备	2	4	6
	综合项目实训	0	4	4
总计		44	56	100

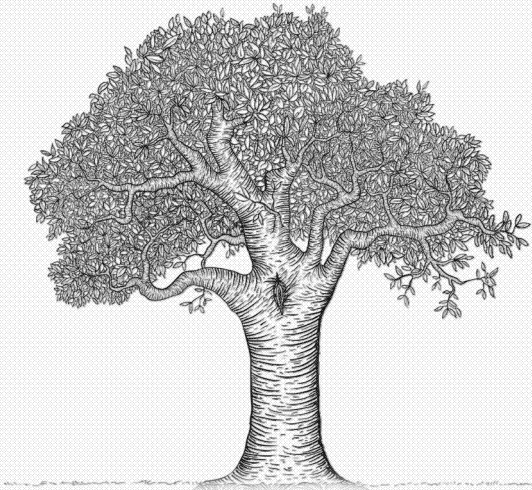
3. 教学资源

为了提高学习效率和教学效果，方便教师教学，编者为本书配备了包括电子教案、教学指南、素材文件、微课，以及习题参考答案等配套的教学资源。请有此需要的读者登录华信教育资源网（<http://www.hxedu.com.cn>）注册后进行免费下载，有问题时请在网站留言板留言或与电子工业出版社联系（E-mail：hxedu@phei.com.cn）。

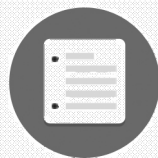
4. 本书作者

本书由余运祥、陆沁、汪双顶主编，由于编者水平有限，加之时间仓促，书中难免有错误和不妥之处，恳请广大师生和读者批评指正。

编 者



CONTENTS | 目录

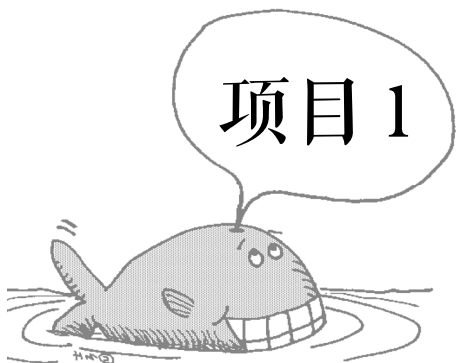


项目1 配置交换机设备	1	【综合实训】：配置路由器	31
任务1 配置交换机	1	任务2 配置路由器的直连路由	32
1.1.1 认识交换机设备	1	2.2.1 路由	32
1.1.2 交换机访问方式	2	2.2.2 直连路由	33
1.1.3 通过带外方式管理交换机	2	【综合实训】：配置直连路由	35
1.1.4 通过带内方式配置交换机	3	任务3 配置路由器的静态路由	36
【综合实训】：配置交换机	4	2.3.1 静态路由	36
任务2 配置虚拟局域网技术	6	2.3.2 默认路由	37
1.2.1 虚拟局域网	6	【综合实训】：配置静态路由和	
1.2.2 虚拟局域网功能	7	默认路由	39
1.2.3 基于端口划分虚拟局域网	8	任务4 配置路由器的 RIP 动态	
1.2.4 虚拟局域网干道技术	9	路由	41
【综合实训】：配置虚拟局域网	10	2.4.1 动态路由	41
任务3 配置交换机生成树技术	13	2.4.2 RIP 协议	42
1.3.1 生成树产生的背景	13	【综合实训】：配置 RIP 路由协议	44
1.3.2 生成树协议	16	项目3 配置三层交换机设备	47
1.3.3 配置交换机简单生成树		任务1 配置三层交换机	47
技术	20	3.1.1 三层交换机	47
1.3.4 配置交换机快速生成树		3.1.2 配置虚拟局域网的 SVI	
技术	21	技术	48
【综合实训】：配置快速生成树	22	3.1.3 配置虚拟局域网单臂路由	
任务4 配置交换机链路聚合技术	23	技术	48
1.4.1 交换机链路聚合技术	23	【综合实训】：配置交换机 SVI	
1.4.2 配置链路聚合技术	25	技术	50
【综合实训】：配置交换机链路		【综合实训】：配置单臂路由	
聚合	26	技术	53
项目2 配置路由器设备	28	任务2 配置三层交换机路由	56
任务1 配置路由器	28	3.2.1 配置三层交换机直连路由	
2.1.1 认识路由器	28	技术	56
2.1.2 配置路由器基础知识	28		



3.2.2 配置三层交换机静态路由技术.....57	【综合实训】：配置路由器 PPP 协议.....95
3.2.3 配置三层交换机 RIP 动态路由技术.....58	任务 2 配置路由器广域网链路认证.....95
【综合实训】：配置三层交换机直连路由.....58	5.2.1 PPP 协议安全认证.....95
【综合实训】：配置三层交换机静态路由.....63	5.2.2 配置 PAP 协议安全认证.....97
【综合实训】：配置三层交换机 RIP 动态路由协议.....65	5.2.3 配置 CHAP 协议安全认证.....98
项目4 配置高级路由技术.....67	【综合实训】：配置 PAP 协议安全认证.....98
任务 1 配置路由器设备链路状态动态路由协议.....67	【综合实训】：配置 CHAP 协议安全认证.....99
4.1.1 链路状态动态路由.....67	任务 3 配置路由器 NAT 技术.....99
4.1.2 OSPF 动态路由协议.....67	5.3.1 路由器 NAT 技术.....99
4.1.3 配置路由设备 OSPF 单区域动态路由协议.....69	5.3.2 路由器 NAPT 技术.....101
4.1.4 配置路由设备 OSPF 多区域动态路由协议.....72	5.3.3 配置路由器 NAT 技术.....102
【综合实训】：配置单区域 OSPF 路由协议.....74	5.3.4 配置路由器 NAPT 技术.....102
【综合实训】：配置多区域 OSPF 路由协议.....78	【综合实训】：配置路由器 NAPT 技术.....103
任务 2 配置路由器路由重发布技术.....81	项目6 配置网络安全技术.....106
4.2.1 路由重发布.....81	任务 1 配置交换机登录安全.....106
4.2.2 使用 RIP 协议的路由重发布.....82	6.1.1 配置交换机控制台密码.....106
4.2.3 使用 OSPF 协议的路由重发布.....83	6.1.2 配置路由器控制台密码.....107
【综合实训】：RIP 中路由重发布.....83	【综合实训】：配置控制台密码.....107
【综合实训】：OSPF 中的路由重发布.....87	任务 2 配置交换机端口安全.....108
项目5 配置路由器接入广域网.....91	6.2.1 配置交换机端口安全.....108
任务 1 配置路由器广域网链路.....91	6.2.2 配置交换机保护端口安全.....110
5.1.1 广域网链路.....91	6.2.3 配置交换机镜像端口安全.....110
5.1.2 配置路由器设备的 PPP 协议.....93	【综合实训】：配置交换机端口安全.....111
	【综合实训】：配置交换机保护端口.....113
	【综合实训】：配置交换机端口镜像.....114
	任务 3 配置编号访问控制列表安全.....115
	6.3.1 配置标准访问控制列表.....115
	6.3.2 配置扩展访问控制列表.....117

6.3.3 配置时间访问控制列表.....117	项目8 配置无线局域网设备.....164
【综合实训】：配置编号标准访问 控制列表.....119	任务1 组建 Ad-Hoc 模式无线 局域网.....164
【综合实训】：配置标准访问控制 列表.....120	8.1.1 无线局域网基础知识.....164
【综合实训】：配置时间访问控制 列表.....121	8.1.2 组建 WLAN 的网络组件.....166
任务4 配置名称访问控制列表.....122	8.1.3 WLAN 的组网模式.....169
6.4.1 配置标准名称访问控制列表 安全.....122	8.1.4 WLAN 的通信协议.....170
6.4.2 配置扩展名称访问控制列表 安全.....123	8.1.5 WLAN 的标识符 SSID.....171
【综合实训】：配置名称访问控制 列表.....123	【综合实训】：组建 Ad-Hoc 模式无线 局域网.....171
项目7 配置防火墙设备.....125	任务2 组建 Infrastructure 模式无线 局域网.....175
任务1 配置防火墙基础技术.....125	8.2.1 Infrastructure 无线网络 基础.....175
7.1.1 防火墙登录配置.....125	8.2.2 胖 AP 基础知识.....176
7.1.2 防火墙初始化配置.....130	8.2.3 瘦 AP 基础知识.....176
【综合实训】：配置防火墙管理员.....131	8.2.4 无线控制器组网知识.....177
【综合实训】：配置防火墙路由 模式.....135	【综合实训】：组建 Infrastructure 模式的无线局域网.....178
任务2 防火墙安全配置.....140	
7.2.1 使用防火墙实现 安全 NAT.....140	
7.2.2 使用防火墙防止 DoS 攻击和 扫描.....142	
7.2.3 配置防火墙用户地址 绑定.....144	
7.2.4 使用防火墙限制连接 带宽.....146	
7.2.5 使用防火墙实现 URL 过滤.....148	
7.2.6 使用防火墙限制 P2P 流量.....151	
7.2.7 配置防火墙链路负载.....153	
【综合实训】：配置防火墙安全 技术.....159	



配置交换机设备

任务 1 配置交换机

1.1.1 认识交换机设备

交换（Switching）是按照通信两端传输信息的需要，用人工或设备自动完成的方法，把要传输的信息送到符合要求的相应路由上的技术的统称。

广义的交换机（Switch）就是一种在通信系统中完成信息交换功能的设备。

普通交换机也称二层交换机，或称为 LAN 交换机，替代集线器优化网络传输效率。像网桥一样，交换机也连接 LAN 分段，利用一张 MAC 地址表来分流帧，从而减少通信量，但交换机的处理速度比网桥快得多。

与网桥相似，二层交换机也是数据链路层设备，能把多个物理上的 LAN 分段，互连成更大的网络。交换机也基于 MAC 地址对通信帧进行转发。由于交换机通过硬件芯片转发，所以交换速度要比网桥软件执行交换快得多。

图 1-1-1 所示是锐捷 RG-S2628G-I 交换机，它具有 24 个百兆端口、4 个千兆端口和 1 个扩展端口插槽，以及 Console 端口（控制口）。此外，它还有一系列的 LED 指示灯。

交换机前面板以太网接口编号由两个部分组成：插槽号和端口在插槽上的编号。默认前面板固化端口插槽编号为 0，端口编号为 3，则该接口书写标识为 FastEthernet0/3。

交换机配置端口是一个特殊端口，是控制交换机设备端口，能实现设备初始化或远程控制。连接 Console 端口需要专用配置线，连接至计算机的 COM 口上，利用终端仿真程序（如 Windows 系统的“超级终端”）进行本地配置。

交换机不配置电源开关，电源接通即可启动。当交换机加电后，前面板 Power 指示灯点亮并呈绿色。前面板上的多排指示灯是端口连接状态灯，代表所有端口的工作状态。



图 1-1-1 锐捷 RG-S2628G-I 系列交换机

交换机是一种智能化的设备，通过配置和管理交换机操作系统，可优化网络传输环境。

1.1.2 交换机访问方式

交换机可以不经任何配置，和集线器一样，加电后直接在局域网内使用。但是这样浪费可管理型交换机提供的智能网络管理功能，局域网内传输效率的优化、各种安全性的提高、网络稳定性、可靠性等也不能实现。因此，需要对交换机进行一定的配置和管理。

对交换机的配置管理，通常通过以下 4 种方式进行。

- 通过带外方式对交换机进行管理。
- 通过 Telnet 对交换机进行远程管理。
- 通过 Web 对交换机进行远程管理。
- 通过 SNMP 管理工作站对交换机进行远程管理。

第一次配置交换机时，只能使用 Console 端口进行配置管理。这种配置方式使用专用的配置线缆，连接交换机 Console 端口并进行配置，不占用网络带宽，因此称为带外管理。其他 3 种方式配置交换机时，均要通过普通网线连接交换机的 FastEthernet 接口，通过 IP 地址实现，因此称为带内方式。交换机连接环境如图 1-1-2 所示。

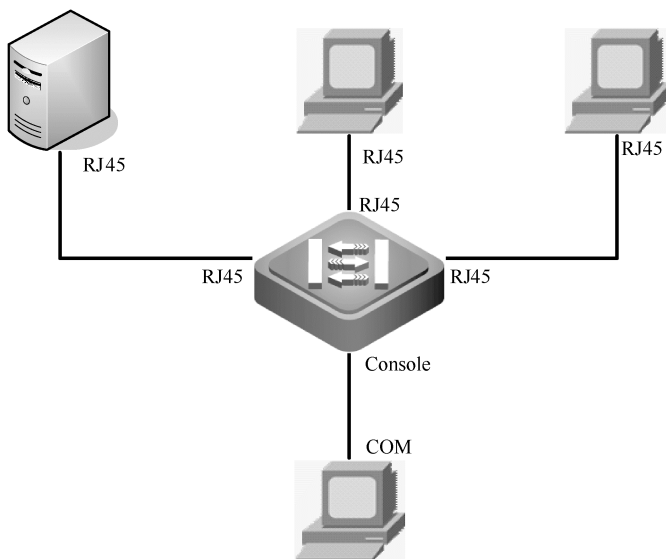


图 1-1-2 交换机的连接环境

1.1.3 通过带外方式管理交换机

不同交换机 Console 端口的位置不同，但该端口都有 Console 标识，如图 1-1-3 所示。利用 Console 线缆，将交换机 Console 口与主机串口连接起来，线缆如图 1-1-4 所示。



图 1-1-3 交换机上的 Console 端口



图 1-1-4 交换机配置线缆

启动交换机，配置计算机上的终端软件程序，如 Windows 系统自带的超级终端程序。

选择“开始”“程序”“附件”“超级终端”命令，按提示配置超级终端程序。

其中，在端口设置时，各项参数如下：每秒位数（波特率）为“9600”，数据位为“8”，奇偶校验为“无”，停止位为“1”，数据流控制为“无”，如图 1-1-5 所示。



图 1-1-5 配置超级终端的端口参数

1.1.4 通过带内方式配置交换机

交换机配置界面分为若干模式，用户所处模式不同，可以使用的命令格式也不同。根据配置管理功能不同，交换机可分为以下 3 种工作模式。

- 用户模式。
- 特权模式。
- 配置模式（全局模式、接口模式、VLAN 模式、线程模式等）。

当用户和设备建立一个会话连接时，首先处于“用户模式”。在用户模式下，只可以使用少量命令，命令的功能也受到限制。

要使用更多配置命令时，必须进入“特权模式”。在特权模式下，用户可使用更多的命令。由此可进入“全局配置模式”，使用配置模式（全局配置模式、接口配置模式等）命令。如用户保存配置信息，这些命令将被保存下来，并在系统重启时，对当前运行配置产生影响。

表 1-1-1 列出了各种命令模式的提示符和示例。



表 1-1-1 交换机各种命令管理模式

用户模式		Switch>提示符	示 例
特权模式		Switch#	Switch>enable
配置模式	全局模式	Switch (config) #	Switch#configure terminal
	VLAN 模式	Switch (config-vlan) #	Switch (config) #vlan 100
	接口模式	Switch (config-if-FastEthernet 0/0) #	Switch (config) #interface fa0/0
	线程模式	Switch (config-line) #	Switch (config) #line console 0

【综合实训】：配置交换机

网络场景

按图 1-1-6 所示网络场景，使用 Console 线缆将交换机 Console 口和计算机上的 COM1 口连接起来。启动计算机超级终端程序，正确配置好参数，实现配置交换机的初始化连接，交换机成功引导之后，进入初始配置。

使用 enable 命令进入特权模式后，再使用 configure terminal 命令进入全局配置模式，就可以开始配置了。



图 1-1-6 网络场景

实施过程

1. 配置交换机名称

```
Ruijie>                                ! 普通用户模式
Ruijie>enable                          ! 进入特权模式
Ruijie# configure terminal             ! 进入全局配置模式
Ruijie (config) # hostname Switch     ! 设置网络设备名称
Switch (config) #                     ! 名称已经修改
```

备注：交换机名称长度不能超过 255 个字符。在全局配置模式下使用“no hostname”命令将系统名称恢复为默认值。

2. 配置系统时间

```
Switch# clock set 05:54:43 1 30 2013 ! 设置系统时间和日期
Switch# show clock                    ! 查看修改系统时间
.....
```

3. 配置每日提示信息

```
Switch(config)# banner motd #                                ! 开始分界符
Enter TEXT message. End with the character '#'.
Notice: system will shutdown on July 6th.#                  ! 结束分界符
Switch(config)#
```

在全局配置模式下，使用“no banner motd”命令，删除配置的每日通知。

4. 配置交换机接口速度

快速以太网交换机端口速度默认为 100Mb/s、全双工。在网络管理工作中，在交换机接口配置模式下，使用以下命令来设置交换机的端口速率。

```
Switch# configure terminal
Switch(config)#interface fastethernet 0/3                  ! F0/3 的端口模式
Switch(config-if-FastEthernet 0/3)#speed 10                ! 配置端口速率为 10Mb/s
! 配置端口速率参数有 100 (100Mb/s)、10 (10Mb/s)、auto (自适应)，默认是 auto
Switch(config-if-FastEthernet 0/3)#duplex half             ! 配置端口的双工模式为半双工
! 配置工式模式有 full (全双工)、half (半双工)、auto (自适应)，默认是 auto
Switch(config-if-FastEthernet 0/3)#no shutdown            ! 开启该端口，转发数据
```

5. 配置交换机管理 IP 地址

二层接口不能配置 IP 地址，可以给交换虚拟接口（Switch Virtual Interface，SVI）配置 IP 地址作为交换机的管理地址。

默认交换虚拟接口 VLAN1 是交换机管理中心，二层交换机管理 IP 地址只能有一个生效。使用以下命令来配置交换机管理 IP 地址。

```
Switch> enable
Switch# configure terminal
Switch (config) # interface vlan 1                          ! 打开 VLAN1 交换机管理中心
Switch (config-if-vlan 1) # ip address 192.168.1.1 255.255.255.0
! 给该交换机配置一个管理地址
Switch (config-if-vlan 1) # no shutdown
Switch (config-if-vlan 1)#end
```

6. 查看并保存配置

在特权模式下，使用“show running-config”命令，查看当前生效配置。如果需要对配置进行保存，可使用“Write”命令保存配置。

```
Switch#show version                                         ! 查看交换机的系统版本信息
.....
Switch#show running-config                                  ! 查看交换机的配置文件信息
.....
Switch#show vlan 1                                          ! 查看交换机的管理中心信息
.....
Switch#show interfaces fa0/1                                ! 查看交换机的 fa0/1 接口信息
.....
```




可以使用以下命令来保存交换机的配置文件信息：

```
Switch # write memory
```

或者：

```
Switch # write
```

或者：

```
Switch# copy running-config startup-config
```

任务 2 配置虚拟局域网技术

1.2.1 虚拟局域网

虚拟局域网（Virtual Local Area Network，VLAN），是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段的技术。这里的网段仅仅是逻辑网段的概念，而不是真正的物理网段。可以将 VLAN 简单地理解为在一个物理网络上逻辑地划分出来的逻辑网络。IEEE 于 1999 年颁布了用以标准化 VLAN 实现方案的 802.1Q 协议标准草案。

VLAN 相当于 OSI 参考模型的第二层的广播域，能够将广播流量控制在一个 VLAN 内部，划分 VLAN 后，由于广播域的缩小，网络中广播包消耗带宽所占的比例大大降低了，网络的性能得到显著提高。不同的 VLAN 之间的数据传输是通过第三层（网络层）的路由来实现的。因此，使用 VLAN 技术，结合数据链路层和网络层的交换设备可搭建安全可靠的网络。

VLAN 与普通局域网最基本的差异体现在：VLAN 并不局限于某一网络或物理范围，VLAN 中的用户可以位于一个园区的任意位置，也可以位于不同的国家。可以根据网络用户的位置、作用、部门或者根据网络用户所使用的应用程序和协议来进行分组，网络管理员通过控制交换机的每一个端口来控制网络用户对网络资源的访问，同时 VLAN 和第三层、第四层的交换结合使用能够为网络提供较好的安全措施。

VLAN 是一组逻辑上的设备和用户，这些设备和用户并不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样。VLAN 是一种比较新的技术，工作在 OSI 参考模型的第二层和第三层，一个 VLAN 就是一个广播域，VLAN 之间的通信是通过第三层的路由器来完成的。

与传统的局域网技术相比较，VLAN 技术更加灵活，它具有以下优点：网络设备的移动、添加和修改的管理开销减少了；可以控制广播活动；可提高网络的安全性。VLAN 是一种将局域网设备从逻辑上划分成一个个网段，从而实现虚拟工作组的新兴数据交换技术。如图 1-2-1 所示，如果不划分 VLAN，那么连接在交换机上的 12 个用户可以直接通信。

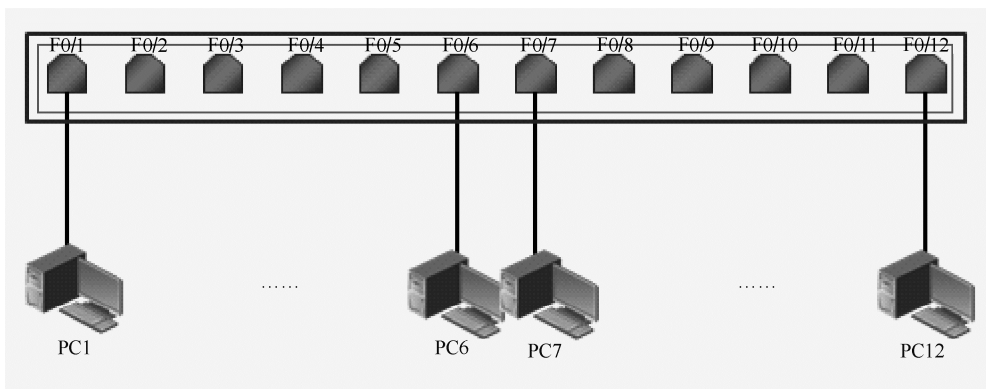


图 1-2-1 VLAN 示意图 1

但如果将 PC1~PC6 划分在一个 VLAN 中，如 VLAN 10；再将 PC7~PC12 划分到另一个 VLAN 中，如 VLAN 20，如图 1-2-2 所示。

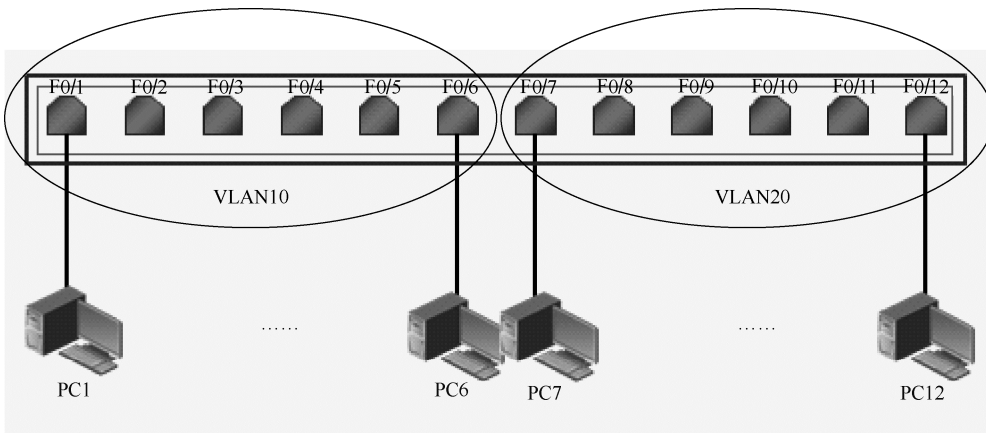


图 1-2-2 VLAN 示意图 2

那么前 6 台 PC，即 PC1~PC6 之间可以通信；后 6 台 PC，即 PC7~PC12 也可以通信，但是前 6 台 PC 和后 6 台 PC，如 PC6 和 PC7 之间无法通信。

简单来说，VLAN 就是将一个物理交换机逻辑地划分成多个小交换机，同一个小交换机的用户可以直接通信，不同逻辑交换机之间无法直接通信。

VLAN 具有以下特点。

- 基于逻辑的分组。
- 在同一 VLAN 内和真实局域网相同。
- 不受物理位置限制。
- 减少结点在网络中移动带来的管理代价。
- 不同 VLAN 内用户要通信需要借助三层设备。

1.2.2 虚拟局域网功能

VLAN 主要有以下两个功能。

- 控制不必要的广播的扩散，从而提高网络带宽利用率，减少资源浪费。



- 划分不同的用户组，对组之间的访问进行限制，从而增加安全性。

默认情况下，交换机所有端口都在一个广播域，也就是说，交换机里一台 PC 发送广播帧，该交换机的其他所有端口都能收到该数据帧。但划分了 VLAN 后，如图 1-2-3 所示，PC1 发送的广播帧到交换机的 F0/1 口后，交换机所有和 F0/1 口在同一个 VLAN 的端口都收到该广播帧，而其他用户无法收到该广播帧，即把一个广播域划分为多个广播域，这样减少了广播帧的洪泛，节省了资源。

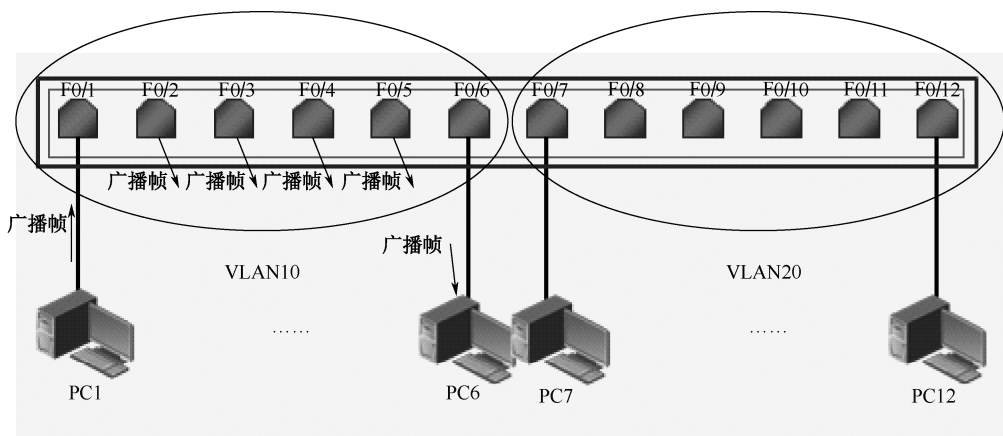


图 1-2-3 交换机中广播传播范围

如果 PC1~PC6 这 6 台 PC 属于公司财务部，而 PC7~PC12 这 6 台 PC 属于公司销售部，这样财务部内部可以互相通信，销售部内部也可以相互通信，而这两个部门之间无法通信。这样可以保证上网用户的安全。

VLAN 的划分方法有以下几种。

- 基于端口的 VLAN：根据以太网交换机的端口来划分 VLAN。
- 基于 MAC 地址的 VLAN：根据每个主机网卡的 MAC 地址来划分 VLAN。
- 基于网络层的 VLAN：根据每个主机的网络层地址或协议类型（如果支持多协议）划分 VLAN。
- 基于 IP 组播的 VLAN：一个组播组就是一个 VLAN。

1.2.3 基于端口划分虚拟局域网

在划分 VLAN 的方法中，最常用的是基于端口的 VLAN 划分。这种划分方法简单实用，就是把交换机的端口划分到对应的 VLAN 中，它实际上是某些交换端口的集合，网络管理员只需要管理和配置交换端口，而不用管交换端口连接什么设备。

这种划分 VLAN 的方法是根据以太网交换机的端口来划分的，例如，划分交换机的 3~8 端口为 VLAN10，19~24 为 VLAN 20。这些属于同一 VLAN 的端口可以不连续，即同一 VLAN 可以跨越数个以太网交换机。

根据端口划分是目前定义 VLAN 最广泛的方法，IEEE 802.1Q 规定了依据以太网交换机的端口来划分 VLAN 的国际标准。这种划分方法的优点是定义 VLAN 成员时非常简单，只要将所有的端口定义一下即可。它的缺点是如果某 VLAN 的用户离开了原来的端口，到了一个新的交换机的某个端口，则必须重新定义。

无论哪些 PC，连接到同一个 VLAN 对应的端口就可以通信，如果连接到不同 VLAN 对

应的端口，则无法正常通信。默认情况下，交换机所有端口都属于 VLAN 1，因此这些端口都可以通信。如图 1-2-4 所示，要将 F0/11、F0/13、F0/15、F0/17 划分到 VLAN 10，将 F0/19、F0/21 ~ F0/24 划分到 VLAN 20，其余端口仍处于 VLAN 1。

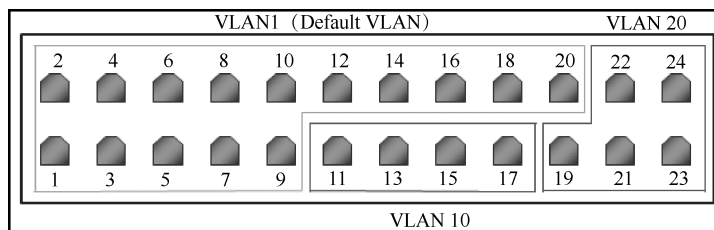


图 1-2-4 VLAN 的划分

如果有 PC1 和 PC2 两台 PC 连接在交换机上：

- PC1 和 PC2 分别连接在 F0/11 和 F0/13 口，两台 PC 可以通信。
- PC1 和 PC2 分别连接在 F0/21 和 F0/22 口，两台 PC 可以通信。
- PC1 和 PC2 分别连接在 F0/1 和 F0/16 口，两台 PC 可以通信。
- PC1 和 PC2 分别连接在 F0/11 和 F0/21 口，两台 PC 不能通信。

配置 VLAN 的思路

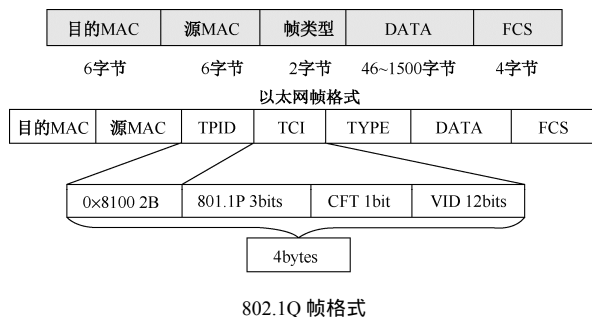
- 创建新 VLAN。
- 手工将端口加入到新 VLAN 中。

1.2.4 虚拟局域网干道技术

在 1996 年 3 月，IEEE 802.1 Internet Working 委员会结束了对 VLAN 初期标准的修订工作。新标准进一步完善了 VLAN 的体系结构，统一了 Frame-Tagging 方式中不同厂商的标签格式，并制定了 802.1Q VLAN 标准。IEEE 802.1Q 使用 4bytes 的标记头定义 TAG（标记），4Bytes 的 TAG 头包括 2Bytes 的 TPID（Tag Protocol Identifier）和 2bytes TCI（Tag Control Information）。其中 TPID 是固定的数值——0×8100。

TCI 包含的组件有：3bits 用户优先级；1bit CFI（Canonical Format Indicator），默认值为 0；12bits 的 VID（VLAN Identifier），即 VLAN 标识符。最多支持 250 个 VLAN，其中 VLAN1 是不可删除的默认 VLAN。

以下是以太网帧格式和 802.1Q 帧格式的比较。



在一台交换机上，同一个 VLAN 间的主机可以通信。

如图 1-2-5 所示，要令两台交换机上相同的 VLAN（如两台交换机上的 VLAN10）可以通



信，则需要将这两台交换机互连起来。一般建议使用干道技术，也就是使用交换机的 TRUNK 口进行互连。

交换机的 TRUNK 口不属于某一个 VLAN 专有，多个 VLAN 的数据可以在 TRUNK 口上同时传输。这和之前说的连接用户的端口不同。之前的连接用户端口只能传输一个 VLAN 的数据，被称为 ACCESS 口。默认情况下，锐捷交换机的所有端口都属于 ACCESS 口。

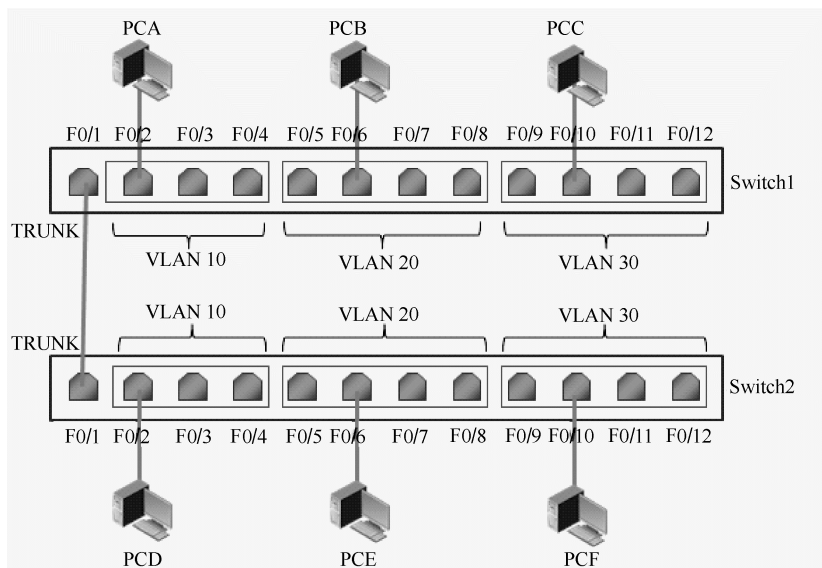


图 1-2-5 TRUNK 互连示意图

由于交换机的 TRUNK 口可以同时传输多个 VLAN 的数据，为了不传错乱，如把 Switch1 内 VLAN 10 的数据传到 Switch2 的 VLAN 20 中，数据在干道上传输时被打上标签，常使用的标签协议是 DOT1Q 协议。如 PCA 发送数据给 PCD，该数据从 Switch1 的 TRUNK 口发出时，会在帧头打上 DOT1Q 的标签，标签内表明该数据属于 VLAN 10。在 Switch2 的 TRUNK 口收到该数据帧后将该标签去除，并将数据发到 VLAN 10 中。

交换机的 TRUNK 口在发送数据时，有一个 VLAN 不打标签，该 VLAN 称为这个 TRUNK 口的 Native VLAN，也称本帧 VLAN。默认交换机 TRUNK 口的本帧 VLAN 是 VLAN 1，可以修改。默认情况下，TRUNK 口允许所有交换机上已经创建的 VLAN 通过。可以通过在交换机的 TRUNK 口上做 VLAN 修剪来过滤不必要的 VLAN 通过。

【综合实训】：配置虚拟局域网

网络场景

按图 1-2-6 所示网络场景是公司办公网络，公司为了减少部门之间的网络干扰，增强部门网络安全性，需要实施部门网络之间的安全隔离，并实现同一部门跨交换机同一虚拟局域网之间的安全连通。

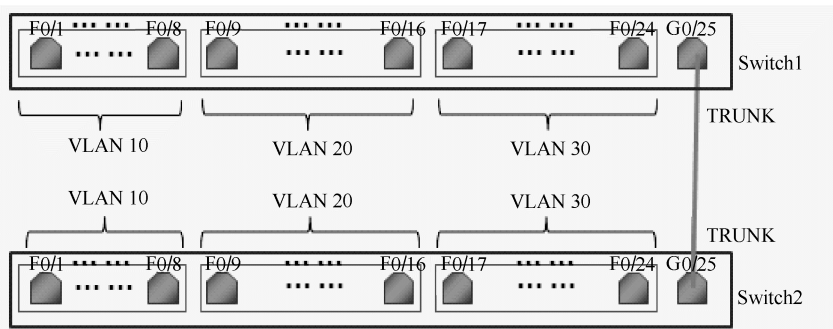


图 1-2-6 场景示意图

实施过程

1. 配置虚拟局域网

➤ Switch1 的配置如下。

```
Ruijie>
Ruijie>enable
Ruijie# configure terminal
Ruijie (config) #hostname switch1
switch1 (config) # vlan 10
switch1 (config-vlan) #exit
switch1 (config) # vlan 20
switch1 (config-vlan) #exit
switch1 (config) # vlan 30
switch1 (config-vlan) #exit
switch1 (config) #
```

! 普通用户模式
! 进入特权模式
! 进入全局配置模式
! 将交换机名称改为 switch1
! 创建 VLAN 10
! 进入全局配置模式
! 创建 VLAN 20
! 进入全局配置模式
! 创建 VLAN 30

➤ Switch2 的配置如下。

```
Ruijie>
Ruijie>enable
Ruijie# configure terminal
Ruijie (config) #hostname switch2
switch2 (config) # vlan 10
switch2 (config-vlan) #exit
switch2 (config) # vlan 20
switch2 (config-vlan) #exit
switch2 (config) # vlan 30
switch2 (config-vlan) #exit
switch2 (config) #
```

! 普通用户模式
! 进入特权模式
! 进入全局配置模式
! 将交换机名称改为 switch2
! 创建 VLAN 10
! 进入全局配置模式
! 创建 VLAN 20
! 进入全局配置模式
! 创建 VLAN 30

备注：为交换机创建 VLAN 时，默认交换机只有 VLAN 1。如果要删除 VLAN，如删除 VLAN 10，则需要输入“no vlan 10”命令。

2. 将接口划分到相应 VLAN

➤ Switch1 的配置如下。

```
switch1 (config) #
switch1 (config) #interface range fa 0/1-8
```

! 进入交换机的 F0/1~F0/8 口



```
switch1 (config-if-range) #switchport access vlan 10    ! 将接口划分到 VLAN 10
switch1 (config-if-range) #exit                          ! 进入全局配置模式
switch1 (config) #interface range fa 0/9-16             ! 进入交换机的 F0/9~F0/16 口
switch1 (config-if-range) #switchport access vlan 20    ! 将接口划分到 VLAN 10
switch1 (config-if-range) #exit                          ! 进入全局配置模式
switch1 (config) #interface range fa 0/17-24            ! 进入交换机的 F0/17~F0/24 口
switch1 (config-if-range) #switchport access vlan 30    ! 将接口划分到 VLAN 30
switch1 (config-if-range) #exit                          ! 进入全局配置模式
switch1 (config) #
```

➤ Switch2 的配置如下。

```
switch2 (config) #
switch2 (config) # interface range fa 0/1-8             ! 进入交换机的 F0/1~F0/8 口
switch2 (config-if-range) #switchport access vlan 10    ! 将接口划分到 VLAN 10
switch2 (config-if-range) #exit                          ! 进入全局配置模式
switch2 (config) #interface range fa 0/9-16             ! 进入交换机的 F0/9~F0/16 口
switch2 (config-if-range) #switchport access vlan 20    ! 将接口划分到 VLAN 10
switch2 (config-if-range) #exit                          ! 进入全局配置模式
switch2 (config) #interface range fa 0/17-24            ! 进入交换机的 F0/17~F0/24 口
switch2 (config-if-range) #switchport access vlan 30    ! 将接口划分到 VLAN 30
switch2 (config-if-range) #exit                          ! 进入全局配置模式
switch2 (config) #
```

备注：锐捷交换机默认所有端口都是 ACCESS 口且属于 VLAN 1。如果先被指定为其他类型，则可以在端口下使用 “switchport mode access” 命令将端口变为 ACCESS 口。

3. 配置交换机的干道技术

➤ Switch1 的配置如下。

```
switch1 (config) #
switch1 (config) #int gi 0/25                          ! 进入 G0/25 口
switch1 (config-if-GigabitEthernet 0/25) #switchport mode trunk
! 将端口变为 TRUNK 口
switch1 (config-if-GigabitEthernet 0/25) #exit          ! 进入全局模式
switch1 (config) #
```

➤ Switch2 的配置如下。

```
switch2 (config) #
switch2 (config) #int gi 0/25                          ! 进入 G0/25 口
switch2 (config-if-GigabitEthernet 0/25) #switchport mode trunk
! 将端口变为 TRUNK 口
switch2 (config-if-GigabitEthernet 0/25) #exit          ! 进入全局模式
switch2 (config) #
```

备注：锐捷交换机端口设置为 TRUNK 口后，默认允许所有已经创建的 VLAN 通过。

4. 配置 TRUNK 口的 VLAN 修剪

➤ Switch1 的配置如下。

```
switch1 (config) #
switch1 (config) #int gi 0/25                          ! 进入 G0/25 口
switch1 (config-if-GigabitEthernet 0/25) #switchport trunk allowed vlan
remove 1-9, 11-19, 21-29, 31-4094
```

! 修剪 TRUNK 口不必要的 VLAN

```
switch1 (config-if-GigabitEthernet 0/25) #exit ! 进入全局模式
switch1 (config) #
```

➤ switch2 的配置如下。

```
switch2 (config) #
switch2 (config) #int gi 0/25 ! 进入 G0/25 口
switch2 (config-if-GigabitEthernet 0/25) #switchport trunk allowed vlan
remove 1-4094
! 先将所有 VLAN 修剪掉
switch2 (config-if-GigabitEthernet 0/25) #switchport trunk allowed vlan add
10, 20, 30
! 添加 VLAN 10, VLAN20, VLAN 30
switch2 (config-if-GigabitEthernet 0/25) #switchport trunk
switch2 (config-if-GigabitEthernet 0/25) #exit ! 进入全局模式
switch2 (config) #
```

备注：在 TRUNK 口下才需进行 VLAN 修剪。修剪时可以将多余 VLAN 修剪掉，也可以先将所有 VLAN 修剪掉，再根据需要增加 VLAN。

5. 保存并查看交换机配置

➤ Switch1 的配置如下。

```
switch1 (config) #
switch1 (config) #end ! 进入交换机特权模式
switch1 #show vlan ! 查看交换机 VLAN 信息
.....
switch1 #show interface switchport ! 查看交换机端口的 VLAN 信息
.....
switch1 #show interface trunk ! 查看交换机端口的干道信息
.....
```

➤ Switch2 的配置如下。

```
switch2 (config) #
switch2 (config) #end ! 进入交换机特权模式
switch2 #show vlan ! 查看交换机 VLAN 信息
.....
switch2 #show interface switchport ! 查看交换机端口的 VLAN 信息
.....
switch2 #show interface trunk ! 查看交换机端口的干道信息
.....
```

任务 3 配置交换机生成树技术

1.3.1 生成树产生的背景

在许多交换机或交换机设备组成的网络环境中，通常使用一些备份连接，以提高网络的健全性、稳定性。备份连接也称备份链路、冗余链路等。备份连接如图 1-3-1 所示，交换机 SW1 与交换机 SW3 的端口 1 之间的链路就是一个备份连接。在主链路（SW1 与 SW2 的端口 2 之间的链路或者 SW2 的端口 1 与 SW3 的端口 2 之间的链路）出现故障时，备份链路自动启



用，从而提高网络的整体可靠性。

使用冗余备份能够为网络带来健全性、稳定性和可靠性等，但是备份链路使网络存在环路。图 1-3-1 中 SW—SW2—SW3 就是一个环路。环路问题是备份链路所面临的最为严重的问题，环路问题将会导致广播风暴、多帧复制及 MAC 地址表的不稳定等问题。

为了减少网络中的单点故障、增加网络可靠性，交换网络中有时会使用冗余拓扑，如图 1-3-1 所示。

正常情况下，PC1 的数据可以从 SW3 的 F0/2 口经 SW2 到达文件服务器。而在 SW3 的 F0/2 口连接线路出现故障时，数据从 SW3 的 F0/1 口经过 SW1 和 SW2 到达服务器。

但冗余拓扑引发的二层环路会带来如下多个问题。

- 广播风暴。
- 多帧复制。
- MAC 地址表抖动。

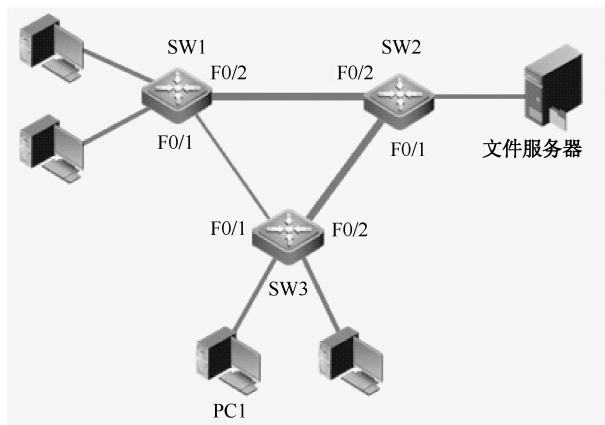


图 1-3-1 交换机冗余拓扑示意图

1. 现象一：广播风暴

在一些较大型的网络中，当大量广播流（如 MAC 地址查询信息等）同时在网络中传播时，便会发生数据包的碰撞。而网络试图缓解这些碰撞并重传更多的数据包，结果导致全网的可用带宽减少，并最终使得网络失去连接而瘫痪。这一过程被称为广播风暴。

网络中，一台设备能够将数据包转发给网络中所有其他站点的技术称为广播。由于广播能够穿越由普通交换机或交换机连接的多个局域网段，因此几乎所有局域网的网络协议都优先使用广播方式来进行管理与操作。广播使用广播帧来发送、传递信息，广播帧没有明确目的地址，发送的对象是网络中的所有主机，也就是说，网络中的所有主机都将接收到该数据帧。

在一个较大规模的网络中，由于拓扑结构的复杂性，会有许多大大小小的环路产生，由于以太网、令牌环网等第二层协议均没有控制环路数据帧的机制，各个小型环路产生的广播风暴将不断扩散到全网，进而造成网络瘫痪。所以广播风暴是二层网络中灾难性的故障。

如图 1-3-2 所示，二层环路导致广播在网络中不停地转发（广播风暴），会瞬间耗尽交换机所有处理能力，使交换机无法转发其他数据。

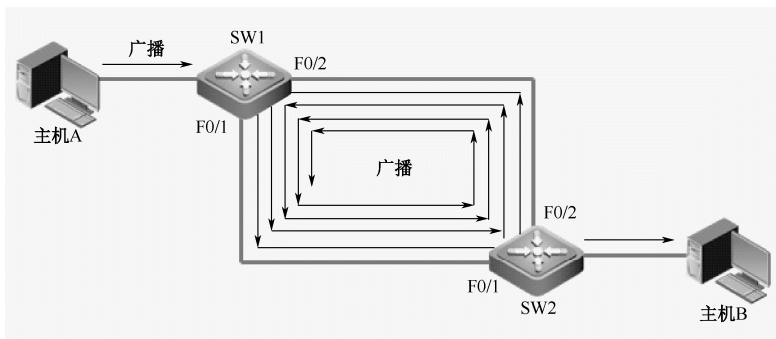


图 1-3-2 广播风暴

2. 现象二：多帧复制

网络中如果存在环路，目的主机可能会收到某个数据帧的多个副本，此时会导致上层协议在处理这些数据帧时无从选择，产生迷惑：究竟该处理哪个帧呢？严重时还可能导致网络连接中断。

如图 1-3-3 所示，二层环路会导致目标结点收到多个相同的数据帧，既浪费结点的处理能力，又浪费网络带宽。

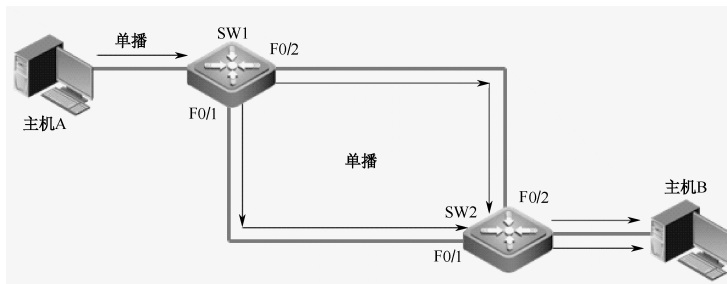


图 1-3-3 多帧复制

3. 现象三：MAC 地址表抖动

当交换机连接不同网段时，将会出现通过不同端口接收到同一个广播帧的多个副本的情况。这一过程也会同时导致 MAC 地址表的多次刷新。这种持续的更新、刷新过程会严重耗用内存资源，影响该交换机的交换能力，同时降低整个网络的运行效率。严重时，将耗尽整个网络资源，并最终造成网络瘫痪。

如图 1-3-4 所示，交换机上的 MAC 地址表不稳定，导致交换机在 MAC 地址表学习上浪费更多资源。所以，网络中的用户需要防止二层环路。其中最常用的方法就是生成树协议。

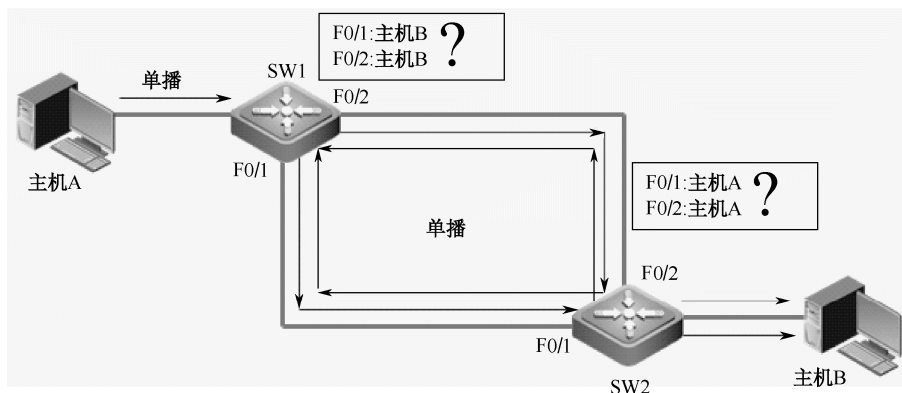


图 1-3-4 MAC 地址抖动

1.3.2 生成树协议

为了解决冗余链路引起的问题，IEEE 通过了 IEEE 802.1d 协议，即生成树协议。IEEE 802.1d 协议通过在交换机上运行一套复杂的算法，使冗余端口置于“阻塞状态”，使得网络中的计算机在通信时，只有一条链路生效，而当这个链路出现故障时，IEEE 802.1d 协议将会重新计算出网络的最优链路，将处于“阻塞状态”的端口重新打开，从而确保网络连接稳定可靠。

1. 生成树概述

生成树协议（Spanning Tree Protocol，STP）最初是由美国数字设备公司（Digital Equipment Corp，DEC）开发的，后经 IEEE 修改，最终制定了相应的 IEEE 802.1d 标准。STP 协议的主要功能就是解决由于备份连接所产生的环路问题。

STP 协议的主要思想就是当网络中存在备份链路时，只允许主链路激活，如果主链路因故障而被断开后，备用链路才会被打开。IEEE 802.1d 生成树协议检测到网络上存在环路时，自动断开环路链路。当交换机间存在多条链路时，交换机的生成树算法只启动最主要的一条链路，而将其他链路都阻塞掉，将这些链路变为备用链路。当主链路出现问题时，生成树协议将自动启用备用链路接替主链路的工作，不需要任何人工干预。

生成树算法的网桥协议 STP 通过将二层网络拓扑从逻辑上转变成树形结构来防止二层环路。

简单来说，生成树的工作原理可以分为以下两步。

- 正常情况下，STP 协议阻塞冗余端口，使网络中结点在通信时，只有一条链路生效。
- 当链路出现故障时，将处于“阻塞状态”的端口重新打开，从而保证网络正常通信。

如图 1-3-5 所示，正常情况下将 SW3 的 F0/1 口逻辑阻塞。这时 SW3 访问 SW2 的数据从 SW3 的 F0/2 口发送到 SW2。当 SW3 的 F0/2 口出现故障后，SW3 的 F0/1 口开始转发数据，SW3 的数据从 F0/1 口经过 SW1 发到 SW2。

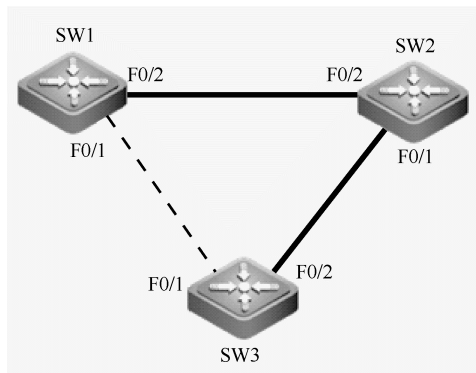


图 1-3-5 生成树工作原理

2. 生成树版本

生成树协议和其他协议一样，是随着网络的不断发展而不断更新换代的。在生成树协议发展过程中，“老旧”的缺陷不断被克服，“新”的特性不断被开发出来。按照功能点的改进情况，可以把生成树协议的发展过程划分成三代。生成树的版本主要有以下三个。

- STP：生成树，标准为 IEEE 802.1d。
- RSTP（Rapid STP）：快速生成树，标准为 IEEE 802.1w。
- MSTP（Multi Instance STP）：多实例生成树，标准为 IEEE 802.1s。

3. 桥协议数据单元

交换机或者网桥之间周期性地发送 STP 的桥接协议数据单元（Bridge Protocol Data Unit，BPDU），用于实现 STP 的功能。

BPDU 主要功能如下。

- 通过比较 BPDU 中的参数得到要阻塞的端口。
- 如果交换机端口在一段时间内未收到 BPDU 报文，则感知到拓扑变化，从而使被阻塞接口转发数据。

BPDU 报文中的主要内容有选举的参数和计时器。

1) 选举参数

- **链路路径开销**：由设备接口带宽换算得出或手工设置，将每段链路的开销累计起来。
- **网桥 ID**：共 64bit，由网桥优先级和网桥 MAC 地址组成。
- **端口 ID**：共 16bit，由端口优先级和端口编号组成。

2) 计时器

- **HELLO TIME**：发送 BPDU 报文的间隔，默认为 2 秒。
- **FORWARD-DELAY TIME**：BPDU 报文传到全网的时间，默认为 15 秒。
- **MAX-AGE TIME**：BPDU 最大生效的时间，默认为 20 秒。

4. 生成树的选举

生成树的选举一般分为以下四步。

(1) 选举一个根网桥。网桥 ID 值最小者当选，如图 1-3-6 所示。

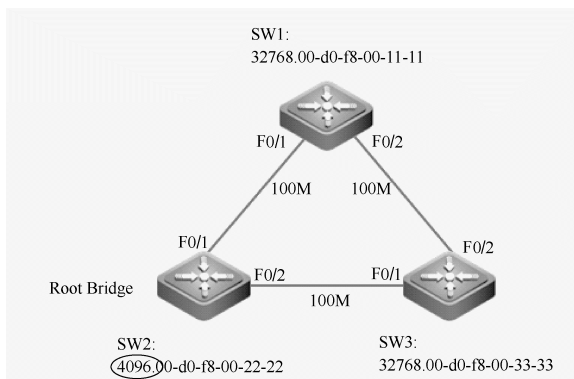


图 1-3-6 选举根网桥

(2) 在每个非根网桥上选举一个根端口，如图 1-3-7 所示。选举依据如下。

- 选择根路径开销最小的端口。
- 如果根路径开销相同，则选择发送网桥 ID 最小的端口。
- 如果发送网桥 ID 相同，则选择发送端口 ID 最小的端口。

(3) 在每个网段上选举一个指定端口，如图 1-3-8 所示。选举依据如下。

- 选择根路径开销最小的端口。
- 如果根路径开销相同，则选择所在交换机的网桥 ID 最小的端口。
- 如果网桥 ID 相同，则选择端口 ID 最小的端口。

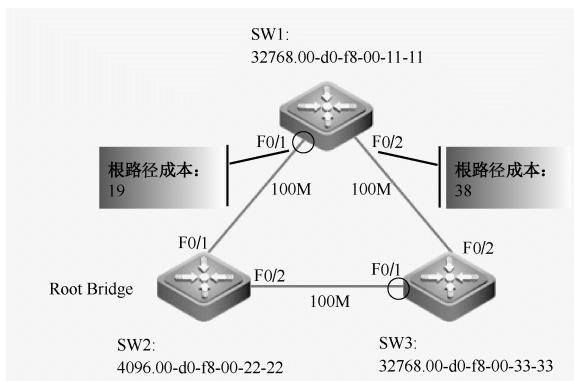


图 1-3-7 选举根端口

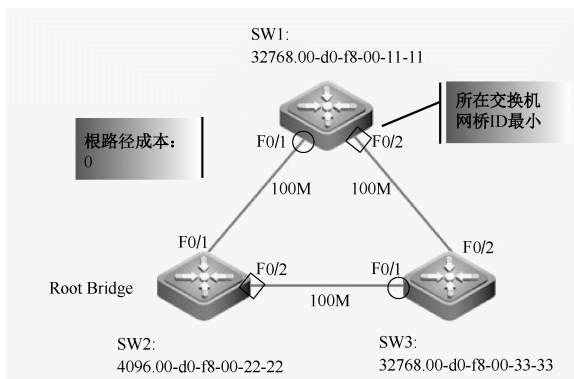


图 1-3-8 选择指定端口

(4) 阻塞非根、非指定端口，如图 1-3-9 所示。

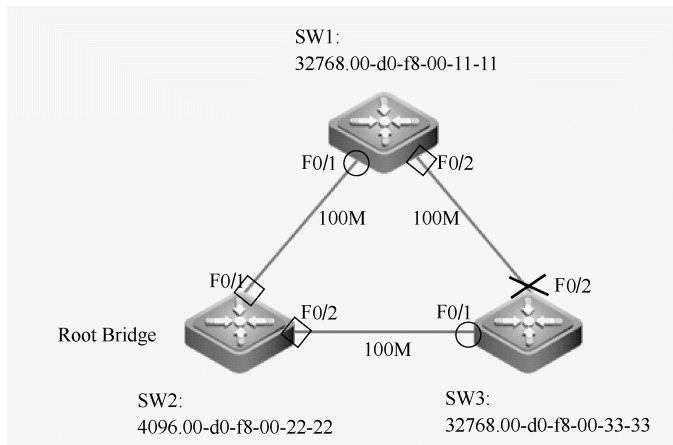


图 1-3-9 生成树选举结果

5. 生成树的接口状态

- **阻塞状态 (Blocking)**：只能接收 BPDU，不能接收或者传输数据，不能把 MAC 地址加入地址表。
- **监听状态 (Listening)**：可以接收和发送 BPDU，不能接收或者传输数据，不能把 MAC 地址加入地址表。
- **学习状态 (Learning)**：可以发送和接收 BPDU，可以学习 MAC 地址，不能传输数据。
- **转发状态 (Forwarding)**：可以发送和接收数据，可以学习 MAC 地址，发送和接收 BPDU。

6. 生成树拓扑变更

生成树拓扑变化示意图如图 1-3-10 所示。

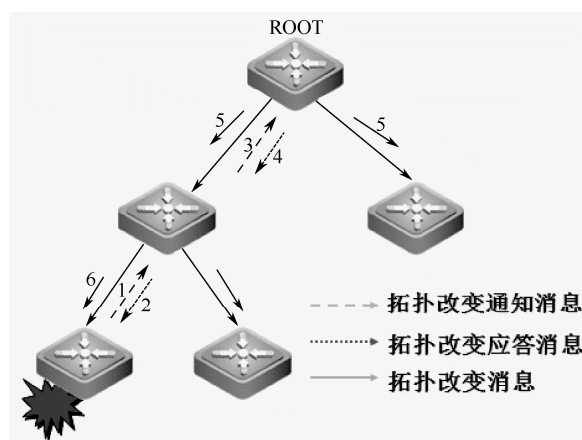


图 1-3-10 生成树拓扑变化示意图

- 由出现链路故障的交换机首先发送拓扑变更报文 (TC)，沿最短路径传递，接收到的交换机回应 (TCA)，直到根交换机为止。



- 根交换机向下发送 TCN 给非根交换机，网络重新计算 STP，从而使网络重新收敛。

7. 快速生成树协议

人们在 IEEE 802.1d 协议的基础之上进行了一些改进，这就产生了 IEEE 802.1w 协议。由于 IEEE 802.1d 通信协议虽然解决了链路闭合引起的死循环问题，但生成树的收敛（指重新设定网络中的交换机端口状态）过程需要的时间比较长，可能需要花费 50s。对于以前的网络来说，50s 的阻断是可以接受的，毕竟那时人们对网络的依赖性不强，但是现在情况不同了，人们对网络的依赖性越来越强，50s 的网络故障足以带来巨大的损失，因此 IEEE 802.1d 协议已经不能适应现代网络的需求了。

快速生成树（Rapid Spanning Tree Protocol，RSTP）与传统的 STP 相比，选举过程基本一致，主要改变是在物理拓扑变化或配置参数发生变化时，能够显著地减少网络拓扑的重新收敛时间。

RSTP 协议在 STP 协议的基础上做了三点重要改进，使得收敛速度快得多（最快 1s 以内）。IEEE 802.1w 协议使收敛过程由原来的 50s 减少为现在的约为 1s，因此 IEEE 802.1w 又称为“快速生成树协议”。

RSTP 收敛快的主要原因有以下几个。

（1）定义了两种新增加的端口角色，用于取代阻塞端口。

- 替代（alternate）端口，也称 AP 端口，为根端口到根网桥的连接提供了替代路径。
- 备份（backup）端口，也称 BP 端口，提供了到达同段网络的备份路径。

（2）端口状态减少为三个。

- 丢弃状态（discarding）：对应 STP 的 disable、blocking、listening 状态。
- 学习（learning）状态。
- 转发（forwarding）状态。

（3）增加了两个变量，用于将端口立即转变为转发状态。

- 边缘端口：指连接终端的端口。
- 连接类型：根据端口的双工模式来确定，全双工操作的端口为点到点链路，可以实现快速收敛。

（4）BPDU 的传播机制改变。

由出现链路故障的交换机首先向相邻交换机发送拓扑变更报文（TCN），收到报文的交换机继续转发，直到收敛。非根网桥即使没有收到根网桥发来的 BPDU，也会每隔 2s 发送一次 BPDU。如果连续 3 个 hello time 里没有收到邻居发来的 BPDU，则认为连接出现故障，重新收敛的时间可能小于 1s。

1.3.3 配置交换机简单生成树技术

对于生成树的配置，最基本的只需要开启生成树，再根据需要选择相应的类型即可。如果需要指定控制选路，则一般只需要修改交换机优先级即可，具体配置如下。

1. 打开 STP 协议

```
Switch(config)# spanning-tree
```

！开启生成树协议

备注：锐捷交换机默认关闭 spanning tree，如果需要关闭生成树协议，则应使用“no spanning-tree”命令。

2. 修改生成树协议的类型

```
Switch(config)#spanning-tree mode stp ! 修改生成树类型
```

3. 配置交换机的优先级

```
Switch(config)#spanning-tree priority <0-61440> ! 修改交换机优先级
```

备注：优先级配置只能为 0 或 4096 的 1~15 倍，默认为 32768。

4. 配置端口的优先级

```
Switch(config-if-FastEthernet 0/1)#spanning-tree port-priority <0-240>  
! 修改端口优先级
```

备注：端口优先级配置只能为 0 或 16 的 1~15 倍，默认为 128。

5. 配置端口的路径成本

```
Switch(config-if-FastEthernet 0/1)#spanning-tree cost cost
```

备注：端口开销默认按接口速率换算。锐捷交换机速率与开销的对应关系如表 1-3-1 所示。

表 1-3-1 锐捷交换机接口速率与开销对应表

接口速率	端口类型	开销
10Mb/s	普通端口	2000000
	Aggregate Link	1900000
100Mb/s	普通端口	200000
	Aggregate Link	190000
1000Mb/s	普通端口	20000
	Aggregate Link	19000

6. 配置 Hello-Time、Forward-delay-Time 和 Max-age-Time

```
Switch(config)#spanning-tree hello-time seconds ! 修改 hello-time  
Switch(config)#spanning-tree forward-time seconds ! 修改 forward-delay-time  
Switch(config)#spanning-tree max-age seconds ! 修改 max-age-time
```

备注：hello time、forward-delay time、max-age time 默认分别为 2s、15s 和 20s。

7. 查看相关命令

```
Switch#show spanning-tree summary ! 查看生成树状态  
Switch#show spanning-tree interface interface-id ! 查看生成树端口状态
```

1.3.4 配置交换机快速生成树技术

快速生成树的配置方法与生成树配置方法类似，其不同点如下。



1. 修改生成树协议的类型

```
Switch(config)#spanning-tree mode rstp
```

! 修改生成树类型

2. 配置边缘端口

```
Switch(config)#int range f 0/1-24
```

! 进入连接终端的接口

```
Switch(config-if-range)#spanning-tree portfast
```

! 将接口设置为边缘端口

备注：如果需要去除边缘端口，则需要输入“spanning-tree portfast disable”。

[综合实训]：配置快速生成树

网络场景

如图 1-3-11 所示，两台计算机分别连接到两台交换机上，两台交换机为了防止单链路故障，而使用了双线连接。交换机配置 RSTP 防环路并将连接计算机的端口配置为 portfast。

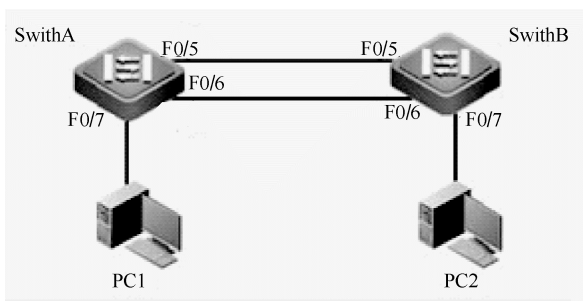


图 1-3-11

实施过程

1. 开启生成树

➤ SwitchA 的配置如下。

```

Ruijie>                                     ! 普通用户模式
Ruijie>enable                               ! 进入特权模式
Ruijie# configure terminal                  ! 进入全局配置模式
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#hostname switchA            ! 设备命名
switchA(config)#spanning-tree              ! 开启生成树协议
switchA(config)#spanning-tree mode rstp    ! 指定生成树类型为快速生成树

```

➤ SwitchB 的配置如下。

```

Ruijie>enable
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#hostname switchB
switchB(config)#spanning-tree

```

```
Enable spanning-tree.
switchB (config) #spanning-tree mode rstp
```

2. 配置快速转发口

➤ SwitchA 上的配置如下。

```
switchA (config) #int fa0/7      ! 进入连接交换机的接口
switchA (config-if-FastEthernet 0/7) #spanning-tree portfast      ! 设置
portfast
%Warning: portfast should only be enabled on ports connected to a
singlehost. Connecting hubs, switches, bridges to this interface when portfast
isenabled, can cause temporary loops.
switchA (config-if-FastEthernet 0/7) #end
```

➤ SwitchB 上的配置如下。

```
switchB (config) #int fa0/7
switchB (config-if-FastEthernet 0/7) #spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a
singlehost. Connecting hubs, switches, bridges to this interface when portfast
isenabled, can cause temporary loops.
switchB (config-if-FastEthernet 0/7) #end
```

3. 查看操作结果

```
switchA#show spanning-tree summary      ! 查看生成树状态
.....
switchA#show spanning-tree interface f 0/5      ! 查看生成树接口
.....
```

任务 4 配置交换机链路聚合技术

1.4.1 交换机链路聚合技术

对于局域网交换机之间以及从交换机到高需求服务的许多网络连接来说，100Mb/s 甚至 1Gb/s 的带宽已经无法满足网络的应用需求。除了 ISP、应用服务提供商、流媒体提供商等企业之外，传统企业网络管理员也会感到自己服务器连接上的带宽压力。

链路聚合技术（也称端口聚合）帮助用户减少了这种压力。制定于 1999 年的 802.3ad 标准定义了如何将两个以上的以太网链路组合起来为高带宽网络连接实现负载共享、负载平衡以及提供更好的冗余性。

如图 1-4-1 所示，可以把多个物理接口捆绑在一起形成一个简单的逻辑接口，这个逻辑接口被称之为一个 Aggregate Port（以下简称 AP）。AP 是链路带宽扩展的一个重要途径，IEEE 802.3ad 符合标准。它可以把多个端口的带宽叠加起来使用，如全双工快速以太网端口形成的 AP 最大传输速度可以达到 800Mb/s，或者千兆以太网接口形成的 AP 最大传输速度可以达到 8Gb/s。



1. 链路聚合

聚合端口基于 IEEE 802.3ad 协议标准。该协议主要用于把多个物理接口捆绑在一起而形成一个逻辑接口。

如图 1-4-1 所示，两台交换机 SW1 和 SW2 上接口最大速率为 1000Mb/s，将 4 个千兆接口进行绑定，两台交换机之间速率可达到 4000Mb/s。

聚合端口优点主要如下。

- 扩展链路带宽。
- 实现成员端口上的流量平衡。
- 自动链路冗余备份。

这项标准适用于 10/100/1000Mb/s 以太网。聚合在一起的链路可以在一条单一逻辑链路上组合使用上述传输速度，这就使用户在交换机之间有一个千兆端口以及 3 或 4 个 100Mb/s 端口时有更多的选择，可以以负担得起的方式逐渐增加带宽。由于网络传输流被动态分布到各个端口，在聚合链路中自动地完成了对实际流经某个端口的数据的管理。

802.3ad 的另一个主要优点是可靠性强。在链路速度可以达到 8Gb/s 的情况下，链路故障将是一场灾难。关键任务交换机链路和服务器连接必须既具有强大的功能又值得信赖。即使在一根电缆被误切断的情况下，也不会瘫痪，这正是 802.3ad 所具有的自动链路冗余备份功能。

这项链路聚合标准在点到点链路上提供了固有的、自动的冗余性。换句话说，如果链路中所使用的多个端口中的一个端口出现故障，网络传输流可以动态地向链路中余下的正常状态的端口进行传输。这种改向速度很快，当交换机得知媒体访问控制地址已经被自动地从一个链路端口重新分配到同一链路中的另一个端口时，改向就被触发。这台交换机将数据发送到新端口位置，并且在服务几乎不中断的情况下，网络继续运行。

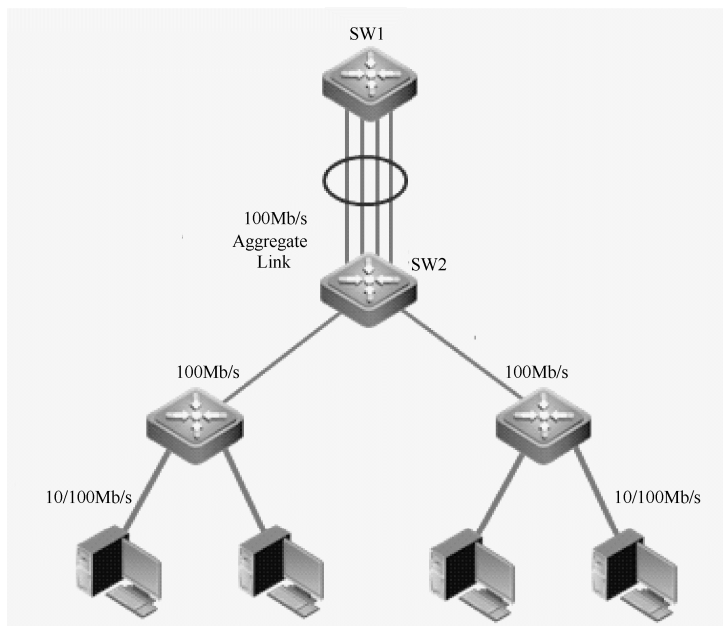


图 1-4-1 聚合端口应用示意图

总之，端口聚合将交换机上的多个端口在物理上连接起来，在逻辑上捆绑在一起，形成

一个拥有较大宽带的端口，形成一条干路，可以实现均衡负载，并提供冗余链路。

2. 流量平衡

AP 根据报文的 MAC 地址或 IP 地址进行流量平衡，即把流量平均地分配到 AP 的成员链路中去。可以根据源 MAC 地址、目的 MAC 地址或源 IP 地址/目的 IP 地址对流量进行平衡。

源 MAC 地址流量平衡即根据报文的源 MAC 地址把报文分配到各个链路中。不同的主机，转发的链路不同，同一台主机的报文，从同一个链路转发（交换机中学到的地址表不会发生变化）。

目的 MAC 地址流量平衡即根据报文的目的 MAC 地址把报文分配到各个链路中。同一目的主机的报文，从同一个链路转发，不同目的主机的报文从不同的链路转发。可以用“aggregateport load-balance”命令设定流量分配方式。

源 IP 地址/目的 IP 地址对流量平衡是根据报文源 IP 与目的 IP 进行流量分配。不同的源 IP/目的 IP 对的报文通过不同的端口转发，同一源 IP/目的 IP 对的报文通过相同的链路转发，其他的源/目的 IP 对的报文通过其他的链路转发。该流量平衡方式一般用于三层 AP。在此流量平衡模式下收到的如果是二层报文，则自动根据源 MAC/目的 MAC 对来进行流量平衡。

流量平衡是把流量平均地分配到 AP 的成员链路中，常见流量平衡方式有以下几种。

- 根据源 MAC 地址实现流量平衡。
- 根据目的 MAC 地址实现流量平衡。
- 根据源 IP 地址实现流量平衡。
- 根据目的 IP 地址实现流量平衡。
- 根据源、目的 MAC 地址实现流量平衡。
- 根据源、目的 IP 地址实现流量平衡。

3. 端口聚合的限制

端口聚合需要满足以下条件。

- AP 成员端口的速率必须一致。
- AP 成员端口必须属于同一个 VLAN。
- AP 成员端口使用的传输介质应相同。
- AP 不能设置端口安全功能。
- AP 成员数量不能超过 8 个。

备注：一个端口加入 AP 后，其端口的属性将被 AP 的属性所取代。将端口从 AP 中删除后，端口的属性将恢复为其加入 AP 前的属性。

1.4.2 配置链路聚合技术

1. 创建链路聚合端口

```
Switch(config)#interface aggregateport n
```

! 创建聚合端口，n 为 AP 号

2. 将链路聚合端口加入 AP

```
Switch(config)#interface range {port-range}
```

! 进入需要聚合的物理接口



```
Switch(config-if-range) # port-group port-group-number ! 将物理接口加入 AP
```

备注：如果这个 AP 不存在，则同时创建这个 AP。

3. 将端口从链路聚合中删除

```
Switch(config-if-FastEthernet 0/1) # no port-group ! 从 AP 中将该成员删除
```

4. 配置链路聚合端口流量平衡

```
Switch(config) # aggregateport load-balance dst-mac ! 按源 MAC 流量平衡
Switch(config) # aggregateport load-balance src-mac ! 按目的 MAC 流量平衡
Switch(config) # aggregateport load-balance src-dst-mac ! 按源和目的 MAC 流量平衡
Switch(config) # aggregateport load-balance dst-ip ! 按目的 IP 流量平衡
Switch(config) # aggregateport load-balance src-ip ! 按源 IP 流量平衡
Switch(config) # aggregateport load-balance ip ! 按源和目的 IP 流量平衡
```

备注：不同型号交换机支持的流量平衡算法可能会有所不同。

5. 查看端口聚合配置

```
Switch# show aggregateport port-number load-balance ! 查看 AP 流量平衡
Switch# show aggregateport port-number summary ! 查看 AP 概述信息
Switch# show interface aggregateport n ! 查看 AP 接口信息
```

【综合实训】：配置交换机链路聚合

网络场景

如图 1-4-2 所示，两台计算机分别连接在两个交换机上，为防单链路故障而使用了双链路互连。由于使用生成树技术使一条链路阻塞，因而使用端口聚合技术且使用基于源 MAC 和目的 MAC 地址实现负载均衡。

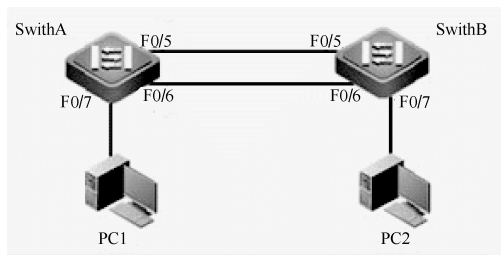


图 1-4-2 交换机链路聚合示意图

实施过程

1. 物理接口加入聚合组

➤ SwitchA 的配置如下。

```
Ruijie>
```

```
! 用户模式
```

```

Ruijie>enable                ! 进入特权模式
Ruijie# configure terminal    ! 进入全局配置模式
Ruijie (config) #hostname switchA    ! 将交换机名称改为 SwitchA
SwitchA (config) #int range f 0/5-6
SwitchA (config-if-range) #port-group 1 ! 将接口加入 aggregateport 1
SwitchA (config-if-range) #exit
SwitchA (config) #

```

➤ SwitchB 的配置如下。

```

Ruijie>en
Ruijie#config t
Ruijie (config) #hostname SwitchB
SwitchB (config) #int ran f 0/5-6
SwitchB (config-if-range) #port-group 1
SwitchB (config-if-range) #exit
SwitchB (config) #

```

2. 配置端口聚合负载均衡

➤ SwitchA 的配置。

```

SwitchA (config) #aggregateport load-balance ?
dst-ip           Destination IP address
dst-mac          Destination MAC address
help            Help information
src-dst-ip       Source and destination IP address
src-dst-ip-l4port Source and destination IP address , source and
                destination L4port
src-dst-mac      Source and destination MAC address
src-ip          Source IP address
src-mac         Source MAC address
src-port        Source port
SwitchA (config) #aggregateport load-balance src-dst-mac
SwitchA (config) #

```

➤ SwitchB 的配置。

```

SwitchB (config) #aggregateport load-balance src-dst-mac
SwitchB (config) #

```

3. 查看实际结果

```

Switch# show aggregateport 1 load-balance    ! 查看 AP 流量平衡
.....
Switch# show aggregateport 1 summary         ! 查看 AP 概述信息
.....
Switch# show interface aggregateport 1      ! 查看 AP 接口信息
.....

```



配置路由器设备

任务1 配置路由器

2.1.1 认识路由器

路由是把信息从源穿过网络传递到目的的行为，在这条路径上，至少遇到一个中间结点。路由发生在第三层（网络层）。路由包含两个基本的动作：确定最佳路径和通过网络传输信息，后者也称为数据转发。数据转发相对来说比较简单，而选择路径很复杂。

路由器（Router）是连接因特网中各局域网、广域网的设备，它会根据信道的情况自动选择和设定路由，并以最佳路径，按前后顺序发送信号的设备。

目前，路由器已经广泛应用于各行各业，各种不同档次的产品已成为实现各种骨干网内部连接、骨干网间互连和骨干网与互连网互联互通业务的主力军。

路由和交换之间的主要区别就是交换发生在OSI 参考模型第二层，即数据链路层。而路由发生在第三层，即网络层。这一区别决定了路由和交换在移动信息的过程中需使用不同的控制信息，所以两者实现各自功能的方式是不同的。

路由器工作主要依据路由表实现。路由器工作过程主要有以下两个。

- （1）生成并维护路由表。
- （2）按路由表转发数据。

如图 2-1-1 所示，路由器和交换机相比，路由器以太网接口数量较少。但大部分路由器有多个扩展槽，从而扩展出多种类型的接口。这些接口大多用来连接广域网。

2.1.2 配置路由器基础知识

1. 路由器管理方式

路由器的管理主要有以下五种方式。

- 通过带外方式对路由器进行管理。
- 通过 Telnet 对路由器进行远程管理。
- 通过 Web 对路由器进行远程管理。
- 通过 SNMP 管理工作站对路由器进行远程管理。
- 通过 AUX 口转换成 Serial 口后通过 Modem 对路由器进行管理。



图 2-1-1 锐捷 RG-RSR20 系列下一代接入路由器

前四种和交换机的使用方法一致，而最后一种方法是路由器特有的。由于目前使用 AUX 接口管理路由器的场景很少，因此这里不再过多介绍。配置访问路由器的方式如图 2-1-2 所示。

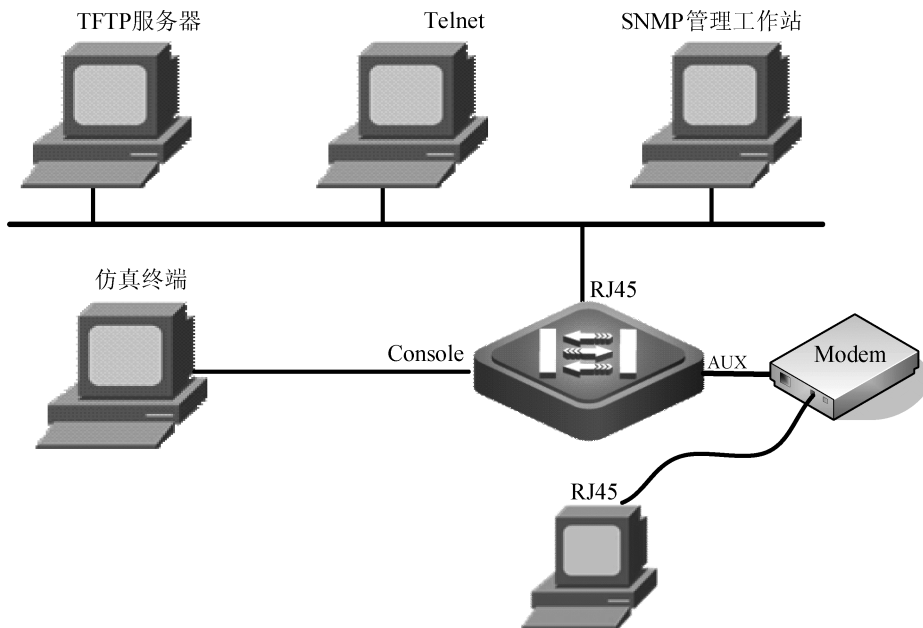


图 2-1-2 配置访问路由器方式

2. 路由器配置界面的模式

由于目前锐捷的交换产品和路由产品基本上都使用统一系统 RGOS 作为设备的操作系统，所以除如 VLAN 模式等交换机特有的模式外，其各种模式的意义和进入的方式与交换机一样，此处不再介绍。

第一次配置路由器时，必须采用 Console 口（也称配置口或控制台口）方式对路由器进行配置，因为这种配置方式通过计算机的串口，直接连接路由器的 Console 口并对其进行配置，不占用网络带宽，因此被称为带外管理，只能在本地配置。



3. 路由器常用命令

除交换机特有的配置，如虚拟局域网、生成树、链路聚合外，路由器和交换机的配置命令基本一样，需要说明的是路由器可以直接在接口上配置 IP 地址。

配置路由器的命令行界面与配置交换机的界面一致，这里不再赘述。表 2-1-1 中列出了路由器命令模式。

表 2-1-1 路由器命令模式

工 作 模 式		提 示 符	启 动 方 式
用户模式		Router>	开机自动进入
特权模式		Router #	Router >enable
配 置 模 式	全局模式	Router (config)#	Router #configure terminal
	路由模式	Router (config-router)#	Router (router)#router rip
	接口模式	Router (config-if)#	Router (config)#interface fa0/0
	线程模式	Router (config-line)#	Router (config)#line console 0

(1) 配置路由器命令行操作模式转换。

```
Router>enable                                ! 进入特权模式
Router#
Router#configure terminal                    ! 进入全局配置模式
Router(config)#

Router(config)#interface fastethernet 1/0    ! 进入路由器 F1/0 接口模式
Router(config-if) #

Router(config-if) #exit                      ! 退回到上一级操作模式
Router(config) #

Router(config-if) #end                       ! 直接退回到特权模式
Router#
```

(2) 配置路由器设备名称。

```
Router> enable
Router# configure terminal
Router(config)#hostname RouterA             ! 把设备的名称修改为 RouterA
RouterA(config)#
```

(3) 显示命令：显示命令就是用于显示某些特定需要的命令，以方便用户查看某些特定设置信息。

```
Router # show version                        ! 查看版本及引导信息
.....
Router # show running-config                ! 查看运行配置
.....
Router # show startup-config                ! 查看保存的配置文件
.....
Router # show interface type number         ! 查看接口信息
.....
Router # show ip route                      ! 查看路由表信息
```

```
.....
Router#write memory                ! 保存当前配置到内存中
Router#copy running-config startup-config
! 保存配置，将当前配置文件复制到初始配置文件中
```

备注：配置文件包含两种类型，即当前正在使用的配置文件 running-config；初始配置文件 startup-config。其中，running-config 保存在 RAM 中，如果没有保存，路由器关机后便丢失；而 startup-config 保存在 NVRAM 中，断电后文件也不会丢失。在系统运行期间，可以随时进入配置模式，对 running-config 进行修改。

【综合实训】：配置路由器

网络场景

如图 2-1-3 所示网络场景，使用 Console 线缆将路由器 Console 口和计算机上的 COM 口进行连接。启动计算机超级终端程序，正确配置好参数，实现配置交换机的初始化连接，路由器成功引导之后，进入初始配置。使用“enable”命令进入特权模式后，再使用“configure terminal”命令进入全局配置模式，就可以开始配置了。

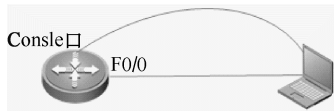


图 2-1-3 路由器连接示意图

实施过程

1. 路由器模式

```
Ruijie>                ! 普通用户模式
Ruijie>enable           ! 进入特权模式
Ruijie# configure terminal ! 进入全局配置模式
Ruijie(config)#hostname router ! 将交换机名称改为 router
```

2. 路由器配置接口 IP

```
router(config)#int f 0/0 ! 进入接口模式
router(config-if-FastEthernet 0/0)#ip address 192.168.1.1 255.255.255.0
! 配置接口 IP 地址及掩码
router(config-if-FastEthernet 0/0)#exit
```

3. 配特权密码

```
router(config)#enable secret ruijie
```

4. 配置远程登录方式

```
router(config)#line vty 0 4
router(config-line)#password dingxiligong
router(config-line)#login
router(config-line)#end
router#
```



5. 查看操作

```
router#show ip int b    ! 接口 IP 配置
.....
router#show int f 0/0    ! 查看接口状态
.....
```

6. 验证

在计算机中选择“开始” “运行”命令，在打开的“运行”对话框中输入“cmd”，在命令窗口中输入“telnet 192.168.1.1”，如图 2-1-4 所示。再输入两级密码后即可登录到路由器中。

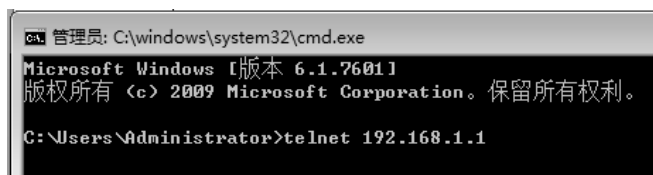


图 2-1-4 Telnet 示意图

任务 2 配置路由器的直连路由

2.2.1 路由

路由就是数据的走向。路由算法根据许多信息来形成路由表，路由信息记录在路由表中，路由表的主要内容是根据目的网段找出数据的下一跳 IP 地址，如图 2-2-1 所示。目的/下一跳地址对告知路由器到达该目的的最佳方式是分组发送给代表“下一跳”的路由器，当路由器收到一个分组后，它会检查其目的地址，尝试将此地址与其“下一跳”相联系。

```
Ruijie#show ip route

Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is 192.168.250.1 to network 0.0.0.0
S    172.16.2.0/24 [1/0] via 192.168.250.1
O    192.168.1.0/24 [110/2] via 192.168.250.1, 00:01:53, GigabitEthernet 0/24
R    192.168.3.0/24 [120/1] via 192.168.250.1, 00:02:07, GigabitEthernet 0/24
C    192.168.250.0/30 is directly connected, GigabitEthernet 0/24
C    192.168.250.2/32 is local host.
```

图 2-2-1 路由表图示

路由表由若干路由条目组成，路由条目有以下字段。

- 目的网段/掩码：表示这个条目对应的地址范围，如果 IP 报文的目的 IP 在这个范围内，则可能会匹配该条目。
- 下一跳 IP：匹配该条目后，数据一般会发到这个 IP 对应的设备。
- 路由来源：常见路由来源如表 2-2-1 所示。

- 管理距离：如果有多条路由条目的目的网段及掩码都相同，此时会比较这个值，值小者优先。每个路由协议默认对应一个管理距离，常见的路由协议默认管理距离如表 2-2-2 所示。

表 2-2-1 路由来源

协 议	标 识
直接路由	C
静态路由/默认路由	S (*)
OSPF	0、0IA、0E2、0E1、0N2、0N1
RTP	R

表 2-2-2 路由协议默认管理距离

协 议	管 理 距 离
直接路由	0
静态路由/默认路由	1
OSPF	110
RTP	120

- 度量值：当路由条目为同一个路由协议时，管理距离默认相同。此时会比较度量值，值小者优先。不同路由协议度量值没有可比性。

路由器查看了数据包的目的 IP 地址后，确定是否知道如何转发该包，如果路由器不知道如何转发，则通常将之丢弃。如果路由器知道如何转发，就把目的物理地址变成下一跳的物理地址并向之发送。下一跳可能就是最终的目的主机，如果不是，通常为另一个路由器，它将执行同样的步骤。当分组在网络中流动时，它的物理地址在改变，但其 IP 地址始终不变。数据在查找路由表转发数据时遵循最长掩码匹配原则。

2.2.2 直连路由

和交换机工作模式不同的是，路由器设备必须经过配置以后，才能开始工作，需要赋予路由器设备的初始配置，其连接网络接口地址，才能保证所连接网络正常通信。

路由器学习路由信息、生成并维护路由表的方法有以下几个。

- 直连路由：路由器接口所连接的子网的路由方式。
- 非直连路由：通过路由协议从其他的路由器学到的路由。非直连路由分为静态路由和动态路由。

路由器各接口直接连接的子网，称为直连网络。直连网络之间使用路由器自动产生的直连路由实现通信。路由表中直连路由信息，在配置完路由器接口 IP 地址后，会自动生成。直连路由是由链路层协议发现的，一般指去往路由器的接口地址所在网段的路径，该路径信息不需要网络管理员维护，也不需要路由器通过某种算法进行计算才能获得，只要该接口处于活动状态，路由器就会把通向该网段的路由信息填写到路由表中，直连路由无法使路由器获取与其不直接相连的路由信息。

直连路由产生的条件如下。

- 接口配置 IP 地址与掩码。
- 接口处于活动状态。

在实际网络中，同一路由器不同接口之间相互通信使用的就是直连路由。如果没有对路



由器接口进行特殊限制，这些接口所直连网络之间，在配置完成地址之后就可以直接通信。一般把这种在路由器接口所连接子网直接配置地址生成的路由方式称为直连路由。直连路由的基本功能就是实现邻居网络之间的互通。图 2-2-2 所示为直连路由场景。

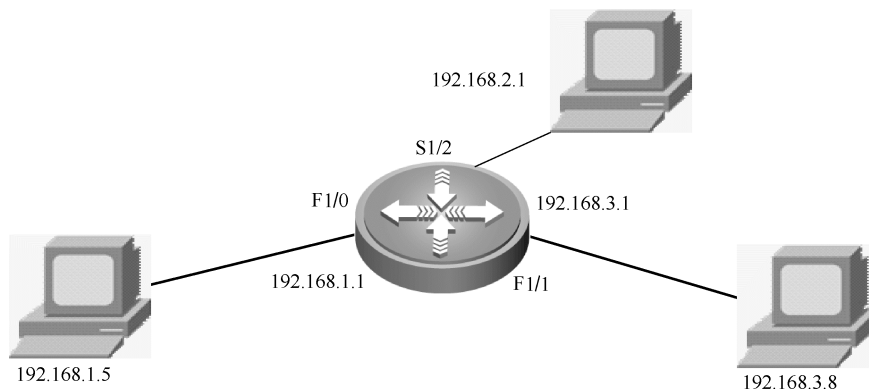


图 2-2-2 路由器接口所连接的直连网络

在直连网络场景中，路由器每个接口单独占用一个子网段地址，配置如表 2-2-3 中的地址后，将自动激活端口所在网段的直连路由，实现这些网段之间的连接。

表 2-2-3 路由器接口所连接的网络地址

接 口	IP 地 址	目 的 网 段
Fastethernet 1/0	192.168.1.1	192.168.1.0
Serial 1/2	192.168.2.1	192.168.2.0
Fastethernet 1/1	192.168.3.1	192.168.3.0

需要通过配置计算机连接到路由器，为所有接口配置所在网络的接口地址，配置方法如下。

```
Router#
Router#configure terminal                ! 进入全局配置模式
Router(config)#
Router(config)#interface fastethernet 1/0    ! 进入路由器 F1/0 接口模式
Router(config-if) #ip address 192.168.1.1 255.255.255.0    ! 配置接口地址
Router(config-if) #no shutdown

Router(config)#interface fastethernet 1/1    ! 进入路由器 F1/1 接口模式
Router(config-if) #ip address 192.168.3.1 255.255.255.0    ! 配置接口地址
Router(config-if) #no shutdown

Router(config)#interface Serial 1/2        ! 进入路由器 Serial 1/2 接口模式
Router(config-if) #ip address 192.168.2.1 255.255.255.0    ! 配置接口地址
Router(config-if) #no shutdown

Router(config-if)#end                    ! 直接退回到特权模式
Router#
```

通过以上配置后，将激活接口，并自动产生直连路由，192.168.1.0 网段被映射到接口 F1/0 上、192.168.2.0 网段被映射到接口 S1/2 上、192.168.3.0 网段被映射到接口 F1/1 上。

【综合实训】：配置直连路由

网络场景

如图 2-2-3 所示，路由器 F0/1 口和 F0/2 口分别连接两台计算机。其中：

PC1 的 IP 地址为 192.168.1.1/24，PC2 的 IP 地址为 192.168.2.2/24，Router 的 F0/1 的 IP 地址为 192.168.1.2/24，F0/2 口为 192.168.2.1/24。

现要求这两台计算机能相互通信。

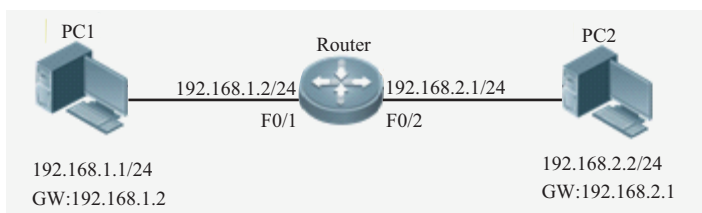


图 2-2-3 直连路由网络图

实施过程

1. 配置 Router 接口的 IP 地址

```
Ruijie>enable                ! 进入特权模式
Ruijie# configure terminal    ! 进入全局配置模式
Ruijie(config)#hostname router
router(config)#int f 0/1
router(config-if-FastEthernet 0/1)#ip address 192.168.1.2 255.255.255.0
router(config-if-FastEthernet 0/1)#exit
router(config)#int f 0/2
router(config-if-FastEthernet 0/2)#ip address 192.168.2.1 255.255.255.0
router(config-if-FastEthernet 0/2)#end
router#
```

2. 计算机配置网关

在 PC1 上配置 IP 地址、子网掩码及网关，如图 2-2-4 所示。

在 PC2 上配置 IP 地址、子网掩码及网关，如图 2-2-5 所示。

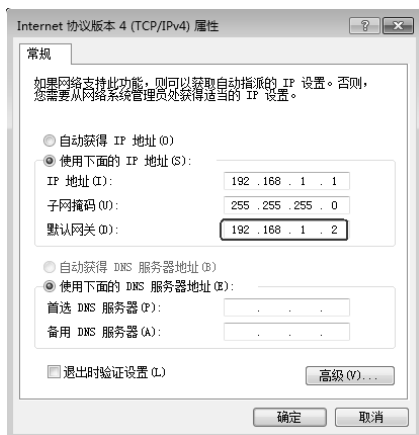


图 2-2-4 PC1 的 IP 地址配置

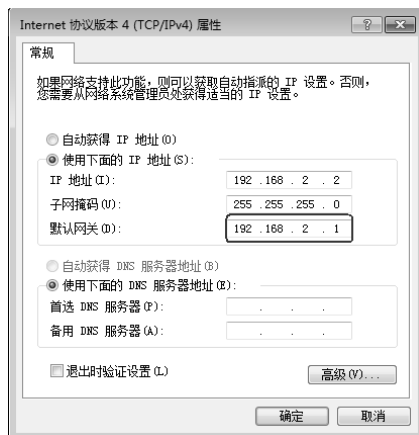


图 2-2-5 PC2 的 IP 地址配置

3. 验证

PC1 和 PC2 能互相 Ping 通。

查看路由表，如图 2-2-6 所示。

```
router#show ip route
```

```
Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set

C    192.168.1.0/24 is directly connected, FastEthernet 0/1
C    192.168.1.2/32 is local host.
C    192.168.2.0/24 is directly connected, FastEthernet 0/2
C    192.168.2.1/32 is local host.
```

图 2-2-6 查看路由表

任务 3 配置路由器的静态路由

2.3.1 静态路由

1. 概述

静态路由是指由管理员手工配置的路由信息。当网络的拓扑结构或链路的状态发生变化时，管理员需要手工去修改路由表中相关的静态路由信息。

当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手工去修改路由表中相关的静态路由信息。静态路由信息在默认情况下是私有的，不会传递给其他的路由器。当然，

网管员也可以通过对路由器进行设置使之成为共享的。静态路由一般适用于比较简单的网络环境，在这样的环境中，网络管理员易于清楚地了解网络的拓扑结构，便于设置正确的路由信息。

静态路由除了具有简单、高效、可靠的优点外，它的另一个好处是网络安全保密性高。动态路由因为需要路由器之间频繁地交换各自的路由表，而对路由表的分析可以揭示网络的拓扑结构和网络地址等信息，因此存在一定的不安全性，而静态路由不存在这样的问题，故出于安全方面的考虑也可以采用静态路由。

大型和复杂的网络环境通常不宜采用静态路由。一方面，网络管理员难以全面地了解整个网络的拓扑结构；另一方面，当网络的拓扑结构和链路状态发生变化时，路由器中的静态路由信息需要大范围地调整，这一工作的难度和复杂程度非常高。

静态路由信息不会传递给其他的路由器。静态路由的优点如下。

- 节省资源，设备间无需发送路由报文。
- 安全性高，设备默认不会把自身的静态路由告诉其他设备。
- 在小型网络中配置简单，易于维护。

静态路由的不足如下。

- 在大型网络中配置复杂。
- 无法自动感知拓扑变化。

静态路由一般适用于比较简单的网络环境，在这样的环境中，网络管理员易于清楚地了解网络的拓扑结构，便于设置正确的路由信息。

2. 配置方法

静态路由的基本配置就是告诉路由器，如果数据要到 A 网段，则把数据给 IP B 对应的设备即可。静态路由的一般配置步骤如下。

- (1) 为每条链路确定地址（包括子网地址和网络地址）。
- (2) 为每个路由器标识非直连的链路地址。
- (3) 为每个路由器写出未直连的地址的路由语句（写出直连地址的语句是没有必要的）。

配置静态路由的命令如下。

```
Ruijie(config)#ip route network-id netmask next-hop-ip
```

有时也可将下一跳 IP 换成输出接口。

对于多个静态路由下一跳 IP 相同且目的网段可以汇总的情况，可以使用汇总的静态路由简化网络的配置。

2.3.2 默认路由

默认路由是一种特殊的静态路由，简单地说，默认路由就是将静态路由的目的网段和子网掩码配置为全 0。这表示无论数据包的目的 IP 是什么，都会将数据发到下一跳 IP 对应的设备。按最长掩码匹配原则，默认路由是最后一步才匹配的。

默认路由通常表示当路由表中没有和包的目的地址匹配的表项时，路由器能够做出的选



择。如果没有默认路由，那么目的地址在路由表中没有匹配表项的包将被丢弃。默认路由在某些时候会大大简化路由器的配置，减轻管理员的工作负担，提高网络性能。

默认路由指的是路由表中未直接列出目的网络的路由选择项，它用于在不明确的情况下指示数据帧下一跳的方向。如果路由器配置了默认路由，则所有未明确指明目的网络的数据包都按默认路由进行转发。

默认路由的使用条件非常苛刻，默认路由一般只使用在 stub 网络中（也称末端网络或存根网络），stub 网络是只有 1 条出口路径的网络，如图 2-3-1 所示。使用默认路由来发送那些目的网络没有包含在路由表中的数据包。

简单地说，默认路由就是在没有找到匹配的路由表入口项时才使用的路由。即只有当没有合适的路由时，默认路由才被使用。在路由表中，默认路由以到网络 0.0.0.0（子网掩码为 0.0.0.0）的路由形式出现。

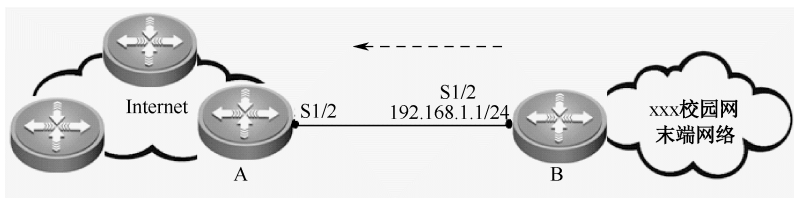


图 2-3-1 默认路由适用的场景

默认情况下，在路由表中直连路由优先级最高，静态路由优先级其次，动态路由优先级再次，默认路由优先级最低！如果没有默认路由，那么目的地址在路由表中没有匹配表项包将被丢弃。

默认路由可以看做静态路由的一种特殊情况。默认路由一般应用在单出口的网络，比如校园网中只有一个 Internet 出口时。

此时，无论是访问哪个运营商的服务器都只能从该出口发送数据。因此可以在出口部署默认路由。默认路由命令如下。

```
Ruijie(config)#ip route 0.0.0.0 0.0.0.0 next-hop-ip
```

在 PC 上，网络中的用户一般除了配置 IP 及掩码外，在跨网段访问时需要配置网关，如图 2-3-2 所示。所谓网关一般就是一个和 PC 的 IP 地址在同一网段的 IP 地址，表示当这台 PC 向其他网段发送数据时，只将数据发给网关对应的设备即可。网络中的用户可以得出网关就是默认路由的下一跳。

二层交换机上也可以配置网关。二层交换机上面的网关不是为下连用户上网提供服务的，而是为二层交换机跨网段通信提供服务。

二层交换机配置网关的命令如下。

```
switch(config)#ip default-gateway gateway
```

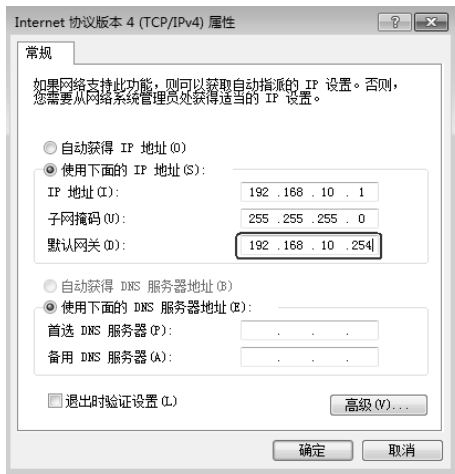


图 2-3-2 计算机网关配置方法

【综合实训】：配置静态路由和默认路由

网络场景

如图 2-3-3 所示，PC1 连接到 Router1 的 F0/0 口，Router1 的 F0/1 口连接到 Router2 的 F0/0 口，Router2 的 F0/1 口连接到 Router3 的 F0/0 口，Router3 的 F0/1 口连接到 PC2。PC1 的 IP 地址为 192.168.1.1/24，网关为 192.168.1.2。

Router1 的 F0/0 口的 IP 地址为 192.168.1.2/24，F0/1 口的 IP 地址为 192.168.2.1/24；Router2 的 F0/0 口的 IP 地址为 192.168.2.2/24，F0/1 口的 IP 地址为 192.168.3.1/24；Router3 的 F0/0 口的 IP 地址为 192.168.3.2/24，F0/1 口的 IP 地址为 192.168.4.1/24；PC2 的 IP 地址为 192.168.4.2/24。

需要通过配置静态路由使 PC1 和 PC2 可以通信。

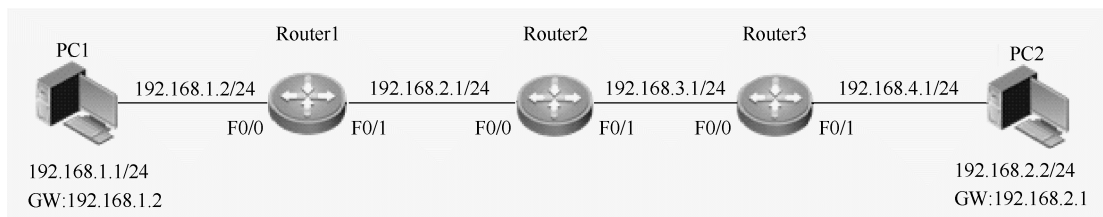


图 2-3-3 静态路由网络拓扑

实施过程

1. 配置接口 IP 地址

➤ Router1 的配置如下。



```
Ruijie#config terminal
Ruijie(config)#hostname router1
router1(config)#int f 0/0
router1(config-if-FastEthernet 0/0)#ip address 192.168.1.2 255.255.255.0
router1(config-if-FastEthernet 0/0)#exit
router1(config)#int f 0/1
router1(config-if-FastEthernet 0/1)#ip address 192.168.2.1 255.255.255.0
router1(config-if-FastEthernet 0/1)#exit
```

➤ Router2 的配置如下。

```
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#hostname router2
router2(config)#int f 0/0
router2(config-if-FastEthernet 0/0)#ip address 192.168.2.2 255.255.255.0
router2(config-if-FastEthernet 0/0)#exit
router2(config)#int f 0/1
router2(config-if-FastEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
router2(config-if-FastEthernet 0/1)#exit
```

➤ Router3 的配置如下。

```
Ruijie#configure
Ruijie(config)#hostname router3
router3(config)#int f 0/0
router3(config-if-FastEthernet 0/0)#ip address 192.168.3.2 255.255.255.0
router3(config-if-FastEthernet 0/0)#exit
router3(config)#int f 0/1
router3(config-if-FastEthernet 0/1)#ip address 192.168.4.1 255.255.255.0
router3(config-if-FastEthernet 0/1)#exit
```

2. 配置静态路由

➤ Router1 的配置如下。

```
router1(config)#ip route 192.168.4.0 255.255.255.0 192.168.2.2
```

➤ Router2 的配置如下。

```
router2(config)#ip route 192.168.4.0 255.255.255.0 192.168.3.2
router2(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1
```

➤ Router3 的配置如下。

```
router3(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1
```

备注：配置静态路由需要双向考虑。

3. PC1 和 PC2 的配置

为 PC1 和 PC2 配置 IP 地址和网关。

4. 验证

PC1 和 PC2 可以相互 Ping 通。

查看路由表，如图 2-3-4 所示。

```
router#show ip route
```

```

router1#show ip route

Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    192.168.1.0/24 is directly connected, FastEthernet 0/0
C    192.168.1.2/32 is local host.
C    192.168.2.0/24 is directly connected, FastEthernet 0/1
C    192.168.2.1/32 is local host.
S    192.168.4.0/24 [1/0] via 192.168.2.2

```

图 2-3-4 静态路由示例

PC1 可以 Ping 通 PC2，但 PC1 不能 Ping 通 192.168.3.2，虽然 PC1 和 PC2 的通信经过 192.168.3.2，如果想让 PC1 Ping 通 192.168.3.2，则可配置静态路由，也可以将 Router1 和 Router3 的静态路由直接改为默认路由，如图 2-3-5 所示。

➤ Router1 的配置如下。

```
router1(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.2
```

➤ Router3 的配置如下。

```
router3(config)#ip route 0.0.0.0 0.0.0.0 192.168.3.1
```

```

router1#show ip route

Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    192.168.1.0/24 is directly connected, FastEthernet 0/0
C    192.168.1.2/32 is local host.
C    192.168.2.0/24 is directly connected, FastEthernet 0/1
C    192.168.2.1/32 is local host.
S*   0.0.0.0/0 [1/0] via 192.168.2.2

```

图 2-3-5 默认路由示意

任务 4 配置路由器的 RIP 动态路由

2.4.1 动态路由

1. 概述

动态路由是指路由器之间能够自动建立自己的路由表，并且能够根据实际情况的变化适时地进行调整。动态路由机制的运作依赖路由器的两个基本功能：对路由表的维护，路由器之间适时的路由信息交换。路由器之间的路由信息交换是基于路由协议实现的。

动态路由表项是通过相互连接的路由器之间交换彼此的信息，然后按照一定的算法优化出来的，而这些路由信息是在一定时间间隙里不断更新的，以适应不断变化的网络，并随时获得最优的寻路效果。



动态路由指路由器能够自动建立自己的路由表，并且能够根据实际情况的变化适时地调整和交换路由信息。交换路由信息的最终目的在于通过路由表找到一条数据交换的“最佳”路径。每一种路由算法都有其衡量“最佳”的一套原则。

大多数算法使用一个量化的参数来衡量路径的优劣，一般来说，参数值越小，路径越好。该参数可以通过路径的某一特性进行计算，也可以在综合多个特性的基础上进行计算。

几个比较常用的特征如下：路径所包含的路由器结点数、网络传输费用、带宽、延迟、负载、可靠性和最大传输单元 MTU (Maximum Transmission Unit , MTU)。

2. 分类

(1) 从运行的范围方面，可分为以下几类。

- 内部网关协议 (IGP)，用来在同一个自治系统内部交换路由信息。典型的内部网关协议有 OSPF、RIP 等。
- 外部网关协议 (EGP)，用来在不同的自治系统间交换路由信息。典型的外部网关协议有 BGP 等。

(2) 从协议的算法方面，可分为以下几类。

- 距离矢量协议，每台路由器在路由信息上都依赖于自己的相邻路由器，而它的相邻路由器又是在它们自己的相邻路由器中学习路由的。典型的距离矢量协议有 RIP 等。
- 链路状态协议，运行链路状态协议的路由器把路由器分成区域，收集区域的所有路由器的链路状态信息，根据状态信息生成网络拓扑结构，每一个路由器再根据拓扑结构计算出路由。典型的链路状态协议有 OSPF 等。

2.4.2 RIP 协议

1. RIP 协议概述

RIP (Routing Information Protocol , 路由信息协议) 是一种古老的基于距离矢量算法的路由协议，通过计算抵达目的地的最少跳数来选取最佳路径。RIP 协议的跳数最多计算到 15 跳，当超过这个数字时，RIP 协议会认为目的地不可达。此外，单纯的以跳数作为选路的依据不能充分描述路径特征，可能导致所选的路径不是最优。因此，RIP 协议只适用于中小型的网络。几乎所有的路由器都支持 RIP 协议。

RIP 是一种内部网关协议，在内部网络上使用。它可以通过不断交换信息让路由器动态地适应网络连接的变化，这些信息包括每个路由器可以到达哪些网络，这些网络有多远等。RIP 属于应用层协议，并使用 UDP 作为传输协议，端口号为 520。

需要注意的是，RIP 协议可能产生环路，因此 RIP 协议有许多防环机制，但仍无法保证其绝对无环。

RIP 协议具有以下特点。

- 路由信息每经过一个路由器，跳数加 1。
- 跳数最小即为最优路由，跳数相同则负载均衡。
- 最多支持的跳数为 15，跳数 16 表示不可达。
- 周期性路由更新，路由会更新为完整的路由表。
- 使用多个时钟以保证路由条目的有效性与及时性。

2. RIP 协议的工作原理

RIP 协议被列为距离矢量，这意味着它使用距离矢量来决定最佳路径，具体来说，它是通过路由跳数来衡量的。路由器每 30s 相互发送广播信息。收到广播信息的每个路由器增加一个跳数。如果广播信息经过多个路由器收到，到这个路由器具有最低跳数的路径是被选中的路径。如果首选的路径不能正常工作，那么其他具有次低跳数的路径（备份路径）将被启用。

RIP 协议基本工作有以下几步。

- （1）运行 RIP 协议的路由器，默认每 30s 广播发送完整的路由表到相邻的 RIP 路由器中。
- （2）相邻路由器学习接收的完整路由表。
- （3）经过 180s 没有收到更新路由就将路由跳数标识为不可达，再经过 120s 还没有收到更新路由就将路由条目删除。

RIP 工作过程如图 2-4-1 所示。

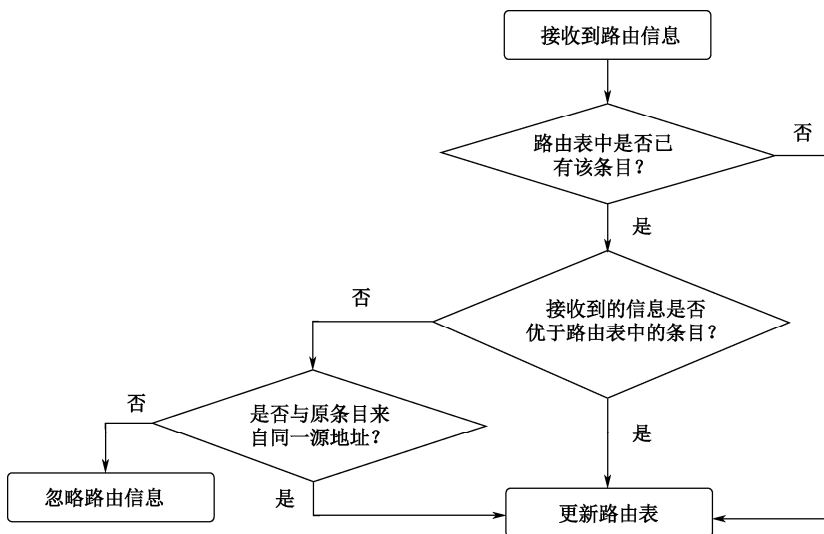


图 2-4-1 RIP 工作过程

3. RIP 的版本

RIP 主要有 v1 和 v2 两个版本，其主要区别如下。

- RIPv1 使用广播方式发送路由更新，RIPv2 使用组播方式发送路由更新。
- RIPv1 路由更新信息中不携带子网掩码，RIPv2 在路由更新中携带子网掩码。
- RIPv1 不支持认证，RIPv2 支持认证。

4. RIP 的路由更新

早期的 RIP 协议中路由的更新是通过定时广播实现的。

默认情况下，路由器每隔 30s 向与它相连的网络广播自己的路由表，接到广播的路由器将收到的信息添加至自身的路由表中。每个路由器都如此广播，最终网络上所有的路由器都会得知全部的路由信息。



正常情况下，每 30s 路由器就可以收到一次路由信息确认，如果经过 180s，即 6 个更新周期，一个路由项还没有得到确认，则路由器认为它已失效了。如果经过 240s，即 8 个更新周期，路由项仍没有得到确认，它会被从路由表中删除。

上面的 30s、180s 和 240s 的延时都是由计时器控制的，它们分别是更新计时器（Update Timer）、无效计时器（Invalid Timer）和刷新计时器（Flush Timer）。

5. RIP 的配置命令

```
Router(config)# router rip          ! 创建路由进程
Router(config-router)# version {1 | 2} ! 指定版本，默认发送 v1 更新包
Router(config-router)# no auto-summary ! 关闭自动汇总功能，默认是开启的
Router(config-router)# network network-number ! 通告直连网段
```

备注：RIP 协议只向直连网络所属接口通告路由信息。

【综合实训】：配置 RIP 路由协议

网络场景

如图 2-4-2 所示，PC1 连接到 Router1 的 F0/0 口，Router1 的 F0/1 口连接到 Router2 的 F0/0 口，Router2 的 F0/1 口连接到 Router3 的 F0/0 口，Router3 的 F0/1 口连接到 PC2。PC1 的 IP 地址为 192.168.1.1/24，网关为 192.168.1.2。

Router1 的 F0/0 口的 IP 地址为 192.168.1.2/24，F0/1 口的 IP 地址为 192.168.2.1/24；Router2 的 F0/0 口的 IP 地址为 192.168.2.2/24，F0/1 口的 IP 地址为 192.168.3.1/24；Router3 的 F0/0 口的 IP 地址为 192.168.3.2/24，F0/1 口的 IP 地址为 192.168.4.1/24；PC2 的 IP 地址为 192.168.4.2/24。

需要通过配置静态路由使 PC1 和 PC2 通信。

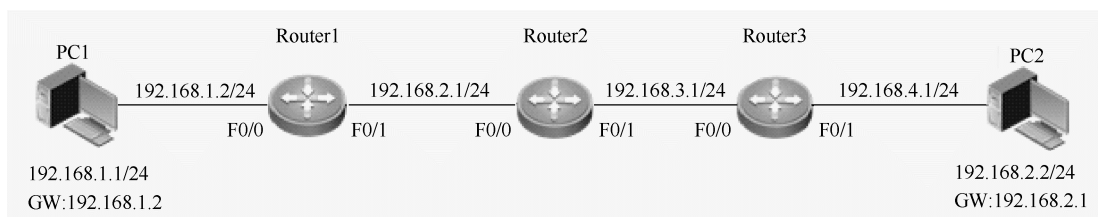


图 2-4-2 RIP 协议拓扑

实施过程

1. 配置接口 IP 地址

➤ Router1 的配置如下。

```
Ruijie#config terminal
Ruijie(config)#hostname router1
router1(config)#int fa0/0
```

```

router1(config-if-FastEthernet 0/0)#ip address 192.168.1.2 255.255.255.0
router1(config-if-FastEthernet 0/0)#exit
router1(config)#int fa 0/1
router1(config-if-FastEthernet 0/1)#ip address 192.168.2.1 255.255.255.0
router1(config-if-FastEthernet 0/1)#exit
router1(config)#

```

➤ Router2 的配置如下。

```

Ruijie#config terminal
Ruijie(config)#hostname router2
router2(config)#int fa 0/0
router2(config-if-FastEthernet 0/0)#ip address 192.168.2.2 255.255.255.0
router2(config-if-FastEthernet 0/0)#exit
router2(config)#int fa 0/1
router2(config-if-FastEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
router2(config-if-FastEthernet 0/1)#exit
router2(config)#

```

➤ Router3 的配置如下。

```

Ruijie#configure terminal
Ruijie(config)#hostname router3
router3(config)#int fa0/0
router3(config-if-FastEthernet 0/0)#ip address 192.168.3.2 255.255.255.0
router3(config-if-FastEthernet 0/0)#exit
router3(config)#int fa0/1
router3(config-if-FastEthernet 0/1)#ip address 192.168.4.1 255.255.255.0
router3(config-if-FastEthernet 0/1)#exit
router3(config)#

```

2. 配置 RIP 协议

➤ Router1 的配置如下。

router1(config)#router rip	! 配置 RIP 进程
router1(config-router)#version 2	! 指定 RIPv2 版本
router1(config-router)#no auto-summary	! 不自动汇总
router1(config-router)#network 192.168.1.0	! 通告直连接口
router1(config-router)#network 192.168.2.0	! 通告直连接口
router1(config-router)#exit	
router1(config)#	

➤ Router2 的配置如下。

```

router2(config)#router rip
router2(config-router)#version 2
router2(config-router)#no auto-summary
router2(config-router)#network 192.168.2.0
router2(config-router)#network 192.168.3.0
router2(config-router)#exit
router2(config)#

```

➤ Router3 的配置如下。

```

router3(config)#router rip
router3(config-router)#version 2
router3(config-router)#no auto-summary
router3(config-router)#network 192.168.3.0
router3(config-router)#network 192.168.4.0

```



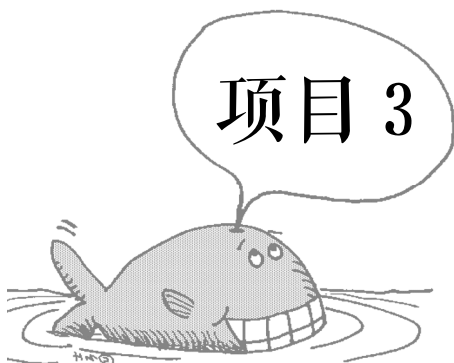

```
router3(config-router)#exit
```

3. PC1 和 PC2 的配置

为 PC1 和 PC2 配置 IP 地址和网关。

4. 验证

PC1 和 PC2 可以相互 Ping 通。此时，可查看路由表信息。



配置三层交换机设备

任务 1 配置三层交换机

3.1.1 三层交换机

三层交换机就是具有部分路由器功能的交换机，三层交换机的最重要目的是加快大型局域网内部的数据交换，所具有的路由功能也是为这个目的服务的，能够做到一次路由，多次转发。对于数据包转发等规律性的过程由硬件高速实现，而像路由信息更新、路由表维护、路由计算、路由确定等功能，由软件实现。

三层交换技术就是二层交换技术加上三层转发技术。传统交换技术是在 OSI 参考模型的数据链路层进行操作的，而三层交换技术是在 OSI 模型中的网络层实现数据包的高速转发的，既可实现网络路由功能，又可根据不同网络状况达到最优网络性能。

如图 3-1-1 所示，三层交换机和二层交换机的物理形态非常类似。对于锐捷交换机来说，名称以“2”开头的交换机属于二层交换机，如 RG-S2628G-E。名称以“2 以上的数”开头的交换机包含了三层交换机的功能。三层交换机中包含路由表。



图 3-1-1 锐捷网络 RG-S3760E 系列交换机



通常情况下，三层交换机可以完成二层交换机的大多数功能，如配置虚拟局域网、生成树、链路聚合等。同时，也可以实现路由器的大多数功能，如配置静态路由协议和大部分动态路由协议。

在校园网中，核心交换机和汇聚交换机一般使用三层交换机。一些银行类用户也越来越喜欢使用三层交换机。

3.1.2 配置虚拟局域网的 SVI 技术

三层交换机有三层功能，可以同时创建多个 IP 地址。但交换机接口默认是二层接口，所以无法直接在接口上配置 IP 地址。

如果需要对接口配置 IP 地址，常用的方法有以下两种。

- 使用路由口。
- 使用 SVI 口。

路由口方式指将三层交换机的二层接口转变成三层接口，这样即可为接口配置 IP 地址了，命令如下。

```
ruijie(config)#interface interface-id ! 进入接口
ruijie(config-if-FastEthernet 0/1)#no switchport ! 将接口配置成路由口
ruijie(config-if-FastEthernet 0/1)#ip address ip-address netmask
! 配置 IP 地址和子网掩码
```

需要注意的是，路由口为三层口，不能将它们配置为 ACCESS 或 TRUNK 等类型的接口。

SVI 口指的是交换机 VLAN 对应的接口，该接口可以配置 IP 地址，再将 VLAN 与物理接口关联。

```
ruijie(config)#vlan vlan-id ! 创建 VLAN
ruijie(config-vlan)#exit ! 进入全局模式
ruijie(config)#int vlan vlan-id ! 创建 SVI
ruijie(config-if-FastEthernet 0/1)#ip address ip-address netmask
! 为 SVI 配置 IP 地址及子网掩码
ruijie(config-if-FastEthernet 0/1)#exit ! 进入全局模式
ruijie(config)#interface interface-id ! 进入物理接口
ruijie(config-if-FastEthernet 0/1)#switchport access vlan vlan-id
! 将物理接口加入 VLAN
```

需要说明的是，在交换机上配置 SVI 可以将交换机的多个 ACCESS 口或 TRUNK 口都加入到该 VLAN 中，此时，这些口都可以使用该 IP 地址。如果在交换机上创建了多个 SVI，并配置了 IP 地址，交换机的 TRUNK 口可以使用多个地址，需要注意干道标签问题。

在校园网中，一般情况下会在汇聚交换机上通过 SVI 方式配置 IP 地址，充当用户和接入层交换机的网关，这样更加灵活。而在汇聚与核心交换机互连时，常使用路由口的方式配置 IP 地址，这样可以防止广播风暴等问题。

3.1.3 配置虚拟局域网单臂路由技术

在交换机不同 VLAN 的用户无法直接通信，如果需要通信则需要借助三层设备。其中，最常见的方式有以下几种。

- 使用三层交换机。在三层交换机上配置 IP 地址，这些 IP 地址可以作为用户网关，通过直连路由进行通信。最常用的是通过 SVI 创建 IP 地址。
- 使用路由器。路由器一般通过单臂路由的方式进行通信。

单臂路由是在路由器的物理接口上创建多个子接口，不同的子接口用于转发不同 VLAN 标签的数据帧，从而实现不同 VLAN 之间的通信。

如图 3-1-2 所示，交换机上配置了 VLAN 10、VLAN 20、VLAN 30 三个 VLAN，每个 VLAN 下包含多个用户。

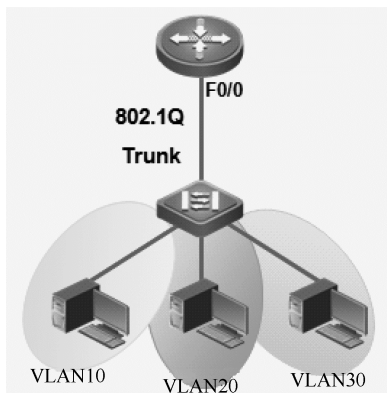


图 3-1-2 单臂路由示意图 1

一般而言，每个 VLAN 对应一个网段，如果要让不同 VLAN 中的用户进行通信，则需要使用路由器实现。可以把交换机上的级联口配置成 TRUNK，在路由器的 F0/0 口上配置子接口。

如图 3-1-3 所示，可将路由器 F0/0 口逻辑地分成三个接口，称为子接口。

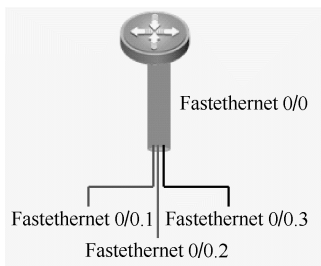


图 3-1-3 单臂路由示意图 2

每个子接口和交换机 VLAN 对应并为每个子接口配置 IP 地址。这些 IP 地址可以充当用户网关，用户通过直连路由进行通信。

配置命令如下。

```
Router(config)#interface type slot-number/interface-number.subinterface-number
! 进入子接口
Router(config-subif)#encapsulation dot1Q VlanID !封装 dot1Q
Router(config-subif)#ip address ip-address mask !配置 IP 地址及子网掩码
```



【综合实训】：配置交换机 SVI 技术

网络场景

如图 3-1-4 所示，学校教学楼汇聚交换机下有一台接入交换机，目前接入交换机 S2628G-I 的 F0/1 和 F0/2 接入 PC1 和 PC2 两个用户，PC3 和 PC4 连接在汇聚交换机 S5750-28GT-L 的 G0/2 和 G0/3 口。接入交换机的 G0/25 口连接到汇聚交换机的 G0/1 口。

楼中有两个部门，出于安全方面的考虑需要把不同部门用户接到不同的 VLAN 中。目前 PC1 和 PC3 在 VLAN 10 中，PC2 和 PC4 在 VLAN 20 中。PC1 的 IP 地址为 192.168.10.1/24，PC2 的 IP 地址为 192.168.20.1/24，PC3 的 IP 地址为 192.168.10.2/24，PC4 的 IP 地址为 192.168.20.2/24。现要求两个部门可以通信。

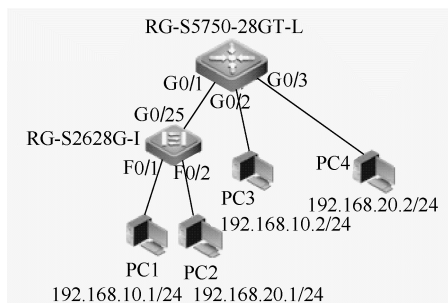


图 3-1-4 SVI 网络示意图

实施过程

1. 划分 VLAN 信息

➤ S5750-28GT-L 的配置如下。

```
Ruijie>en
Ruijie#config t
Ruijie(config)#hostname huiju
huiju(config)#vlan 10
huiju(config-vlan)#exit
huiju(config)#vlan 20
huiju(config-vlan)#exit
huiju(config)#int g 0/1
huiju(config-if-GigabitEthernet 0/1)#switchport mode trunk
! 将 G0/1 配置为 trunk
huiju(config-if-GigabitEthernet 0/1)#swi tru all vlan remove 1-9,11-19,21-4094
! 给 G0/1 口进行 VLAN 修剪
huiju(config-if-GigabitEthernet 0/1)#exit
huiju(config)#int g 0/2
huiju(config-if-GigabitEthernet 0/2)#switchport access vlan 10
huiju(config-if-GigabitEthernet 0/2)#exi
```

```
huiju(config)#int g 0/3
huiju(config-if-GigabitEthernet 0/3)#switchport access vlan 20
huiju(config-if-GigabitEthernet 0/3)#exit
huiju(config)#
```

备注：接入交换机上配置多个 VLAN，接入交换机和汇聚交换机使用 TRUNK 互连。

➤ S2628G-I 的配置如下。

```
Ruijie#config t
Ruijie(config)#hostname jieru
jieru(config)#vlan 10
jieru(config-vlan)#exit
jieru(config)#vlan 20
jieru(config-vlan)#exit
jieru(config)#int f 0/1
jieru(config-if-FastEthernet 0/1)#switchport access vlan 10
jieru(config-if-FastEthernet 0/1)#exit
jieru(config)#int f 0/2
jieru(config-if-FastEthernet 0/2)#switchport access vlan 20
jieru(config-if-FastEthernet 0/2)#exit
jieru(config)#int gi 0/25
jieru(config-if-GigabitEthernet 0/25)#switchport mode trunk
jieru(config-if-GigabitEthernet 0/25)#swi trunk al vl rem 1-9,11-19,21-4094
jieru(config-if-GigabitEthernet 0/25)#exit
```

2. 为 PC 配置 IP 地址及网关

PC1：IP 地址为 192.168.10.1/24，网关为 192.168.10.254。

PC2：IP 地址为 192.168.20.1/24，网关为 192.168.20.254。

PC3：IP 地址为 192.168.10.2/24，网关为 192.168.10.254。

PC4：IP 地址为 192.168.20.2/24，网关为 192.168.20.254。

备注：此时无论网关是否配置，PC1 和 PC3 都可以通信，PC2 和 PC4 都可以通信，但是 PC1 和 PC3 虽属于同一个交换机，但因隶属于不同 VLAN 而不能通信，PC2 和 PC4 也不能通信。

3. 在三层交换机配置 SVI 实现不同 VLAN 通信

```
huiju(config)#int vlan 10
huiju(config-if-VLAN 10)#ip address 192.168.10.254 255.255.255.0
! 该 SVI 充当 VLAN 10 用户的网关
huiju(config-if-VLAN 10)#exit
huiju(config)#int vlan 20
huiju(config-if-VLAN 20)# ip address 192.168.20.254 255.255.255.0
! 该 SVI 充当 VLAN 20 用户的网关
huiju(config-if-VLAN 20)#exit
```

备注：创建 SVI 要先创建 VLAN，如果不创建 VLAN 则无法创建 SVI。三层交换机可配置多个 SVI。

4. 验证

(1) 使用不同 PC 相互 Ping，此时 PC1、PC2、PC3、PC4 之间都可以互通。

(2) 查看三层交换机的 SVI 信息，如图 3-1-5 所示。

查看三层地址，命令如下。



```
huiju#show ip int b
```

```
huiju#show ip int b
```

Interface	IP-Address(Pri)	OK?	Status
VLAN 10	192.168.10.254/24	YES	UP
VLAN 20	192.168.20.254/24	YES	UP

图 3-1-5 SVI 地址信息

查看接口状态，如图 3-1-6 和图 3-1-7 所示。

```
huiju#show int vlan vlan-id
```

```
huiju#show int vlan 10
```

```
Index(dec):4106 (hex):100a
```

```
VLAN 10 is UP , line protocol is UP
```

```
Hardware is VLAN, address is 1414.4b5d.875e (bia 1414.4b5d.875e)
```

```
Interface address is: 192.168.10.254/24
```

```
ARP type: ARPA, ARP Timeout: 3600 seconds
```

```
MTU 1500 bytes, BW 1000000 Kbit
```

```
Encapsulation protocol is Ethernet-II, loopback not set
```

```
Keepalive interval is 10 sec, set
```

```
Carrier delay is 2 sec
```

```
Rxload is 1/255, Txload is 1/255
```

图 3-1-6 Interface VLAN 10 接口状态信息

```
huiju#show int vlan 20
```

```
Index(dec):4116 (hex):1014
```

```
VLAN 20 is UP , line protocol is UP
```

```
Hardware is VLAN, address is 1414.4b5d.875e (bia 1414.4b5d.875e)
```

```
Interface address is: 192.168.20.254/24
```

```
ARP type: ARPA, ARP Timeout: 3600 seconds
```

```
MTU 1500 bytes, BW 1000000 Kbit
```

```
Encapsulation protocol is Ethernet-II, loopback not set
```

```
Keepalive interval is 10 sec, set
```

```
Carrier delay is 2 sec
```

```
Rxload is 1/255, Txload is 1/255
```

图 3-1-7 Interface VLAN 20 接口状态信息

备注：使用 SVI 时要注意接口状态必须为 UP，否则无法正常使用。三层交换机不同 SVI 的 IP 地址不在同一个网段，锐捷三层交换机通过虚拟技术使得不同 SVI 的 MAC 地址相同。

【综合实训】：配置单臂路由技术

网络场景

如图 3-1-8 所示，PC1、PC2、PC3 连接在二层交换机 S2628G-I 下，由于这三台计算机属于不同部门，因此将它们划分到不同 VLAN 中，其中 PC1 在 VLAN 10 中，PC2 在 VLAN 20 中，PC3 在 VLAN 30 中。要令这三台 PC 相互通信，因此在网络中部署了一台路由器，路由器的 F0/0 口连接到二层交换机的 G0/25 中。

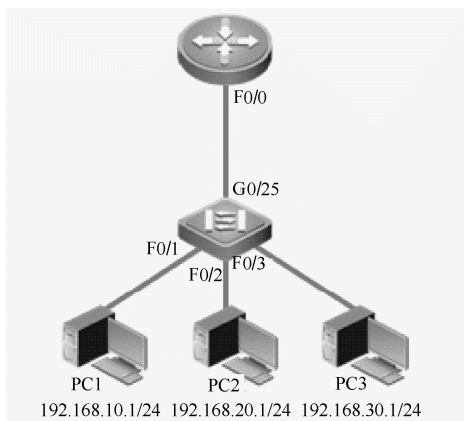


图 3-1-8 单臂路由

实施过程

1. 配置 PC 的 IP 地址和网关

PC1 的 IP 地址为 192.168.10.1/24，网关为 192.168.10.254。

PC2 的 IP 地址为 192.168.20.1/24，网关为 192.168.20.254。

PC3 的 IP 地址为 192.168.30.1/24，网关为 192.168.30.254。

2. 配置二层交换机 VLAN 信息

```
Ruijie#config t
Ruijie(config)#hostname switch
switch(config)#vlan 10
switch(config-vlan)#exi
switch(config)#vlan 20
switch(config-vlan)#exit
switch(config)#vlan 30
switch(config-vlan)#exit
switch(config)#int f 0/1
switch(config-if-FastEthernet 0/1)#switchport access vlan 10
switch(config-if-FastEthernet 0/1)#exi
switch(config)#int f 0/2
```




```
switch(config-if-FastEthernet 0/2)#switchport access vlan 20
switch(config-if-FastEthernet 0/2)#exit
switch(config)#int f 0/3
switch(config-if-FastEthernet 0/3)#switchport access vlan 30
switch(config-if-FastEthernet 0/3)#exit
switch(config)#
```

备注：此时无论 PC 是否配置网关，不同 VLAN 间无法正常通信。

3. 配置三层信息

➤ Switch 的配置如下。

```
switch(config)#int gi 0/25
switch(config-if-GigabitEthernet 0/25)#switchport mode trunk
switch(config-if-GigabitEthernet 0/25)#exit
switch(config)#
```

备注：由于三个 VLAN 都需要通过这个接口连接到路由器，因此要将该接口配置为 TRUNK。

➤ Router 的配置如下。

```
Ruijie>
Ruijie>en
Ruijie#config t
Ruijie(config)#hostname router
router(config)#int f 0/0.1                ! 进入 F0/0 对应的子接口
router(config-subif)#encapsulation dot1q 10    ! 子接口关联到 VLAN
router(config-subif)#ip address 192.168.10.254 255.255.255.0
! 子接口配置 IP 地址及子网掩码
router(config-subif)#exit
router(config)#int f 0/0.2
router(config-subif)#encapsulation dot1q 20
router(config-subif)#ip address 192.168.20.254 255.255.255.0
router(config-subif)#exit
router(config)#int f 0/0.3
router(config-subif)#encapsulation dot1q 30
router(config-subif)#ip address 192.168.30.254 255.255.255.0
router(config-subif)#exit
router(config)#
```

备注：配置子接口时一般先保证主接口下没有配置 IP 地址。在创建子接口时，不需要按顺序从小到大创建。

不同子接口要保证对应不同的 dot1q，以为每个子接口下配置的 IP 地址充当用户网关，不同子接口的 IP 地址不在同一网段。

4. 验证

(1) PC1、PC2、PC3 之间可以相互 Ping 通。

(2) 查看路由器信息。

查看路由表，如图 3-1-9 所示。

```
router#show ip route
```

```

router#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set

C    192.168.10.0/24 is directly connected, FastEthernet 0/0.1
C    192.168.10.254/32 is local host.
C    192.168.20.0/24 is directly connected, FastEthernet 0/0.2
C    192.168.20.254/32 is local host.
C    192.168.30.0/24 is directly connected, FastEthernet 0/0.3
C    192.168.30.254/32 is local host.

```

图 3-1-9 路由器的路由表信息

查看路由器三层地址信息，如图 3-1-10 所示。

```
router#show ip int b
```

备注：主接口下没有 IP 地址。

```

router#show ip int b
Interface                IP-Address(Pri)      IP-Address(Sec)      Status    Protocol
FastEthernet 0/0.3       192.168.30.254/24    no address            up        up
FastEthernet 0/0.2       192.168.20.254/24    no address            up        up
FastEthernet 0/0.1       192.168.10.254/24    no address            up        up
FastEthernet 0/0         no address            no address            up        down
FastEthernet 0/1         no address            no address            up        down
FastEthernet 0/2         no address            no address            up        down

```

图 3-1-10 路由器三层地址信息

查看路由器子接口信息，如图 3-1-11 ~ 图 3-1-14 所示。

```
router#show interface interface-id
```

备注：F0/0 子接口的 MAC 地址与自身相同。

```

router#show int f0/0
Index(dec):1 (hex):1
FastEthernet 0/0 is UP, line protocol is UP
Hardware is MPC8248 FCC FAST ETHERNET CONTROLLER FastEthernet, address is 1414.4b67.f97c
(bia 1414.4b67.f97c)
Interface address is: no ip address
ARP type: ARPA, ARP Timeout: 3600 seconds
MTU 1500 bytes, BW 100000 Kbit
Encapsulation protocol is Ethernet-II, loopback not set

```

图 3-1-11 F0/0 的信息



```
router#show interface f 0/0.1↵  
ifindex(dec):5 (hex):5↵  
FastEthernet 0/0.1 is UP , line protocol is UP ↵  
Hardware is MPC8248 FCC FAST ETHERNET CONTROLLER FastEthernet, address is  
1414.4b67.f97c (bia 1414.4b67.f97c)↵  
Interface address is: 192.168.10.254/24↵  
ARP type: ARPA,ARP Timeout: 3600 seconds↵  
MTU 1500 bytes, BW 100000 Kbit↵  
Encapsulation protocol is 802.1Q Virtual LAN,Vlan ID 10↵
```

图 3-1-12 F0/1 的信息

```
router#show int f0/0.2↵  
ifindex(dec):6 (hex):6↵  
FastEthernet 0/0.2 is UP , line protocol is UP ↵  
Hardware is MPC8248 FCC FAST ETHERNET CONTROLLER FastEthernet, address is  
1414.4b67.f97c (bia 1414.4b67.f97c)↵  
Interface address is: 192.168.20.254/24↵  
ARP type: ARPA,ARP Timeout: 3600 seconds↵  
MTU 1500 bytes, BW 100000 Kbit↵  
Encapsulation protocol is 802.1Q Virtual LAN,Vlan ID 20↵
```

图 3-1-13 F0/2 的信息

```
router#show int f 0/0.3↵  
ifindex(dec):7 (hex):7↵  
FastEthernet 0/0.3 is UP , line protocol is UP ↵  
Hardware is MPC8248 FCC FAST ETHERNET CONTROLLER FastEthernet, address is  
1414.4b67.f97c (bia 1414.4b67.f97c)↵  
Interface address is: 192.168.30.254/24↵  
ARP type: ARPA,ARP Timeout: 3600 seconds↵  
MTU 1500 bytes, BW 100000 Kbit↵  
Encapsulation protocol is 802.1Q Virtual LAN,Vlan ID 30↵
```

图 3-1-14 F0/3 的信息

任务 2 配置三层交换机路由

3.2.1 配置三层交换机直连路由技术

1. 概述

三层交换机的直连路由技术与路由器类似。但三层交换机可以通过路由口和 SVI 两种方

式配置直连路由，而路由器不能使用 SVI 方式。

如图 3-2-1 所示，三层交换机通过 SVI 配置 IP 地址后，在路由表中直连路由对应的出接口为 SVI 口。此时，如果数据需要从该接口发出，则需要通过 SVI 找到对应的物理接口。如果交换机多个接口都属于该 VLAN，则需要查询 MAC 地址表找到该物理接口，将数据从该接口发出。而对于路由器来说，其不同接口对应不同网段，因此可以通过路由表直接发送数据。

```
Codes: C - connected, S - static, R - RIPv1, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
Gateway of last resort is not set
C 192.168.10.0/24 is directly connected, VLAN 10
C 192.168.10.1/32 is local host.
C 192.168.20.0/24 is directly connected, VLAN 20
C 192.168.20.1/32 is local host.
C 192.168.30.0/24 is directly connected, VLAN 30
C 192.168.30.1/32 is local host.
```

图 3-2-1 三层交换机直连路由

三层交换机 SVI 对应的直连路由生效的前提如下。

- SVI 配置了有效的 IP 地址。
- SVI 口 UP。SVI 口 UP 的条件是 VLAN 至少包含一个 UP 的物理接口。

2. 三层交换机互连方式

如图 3-2-2 所示，三层交换机常见接口互连的方式如下。

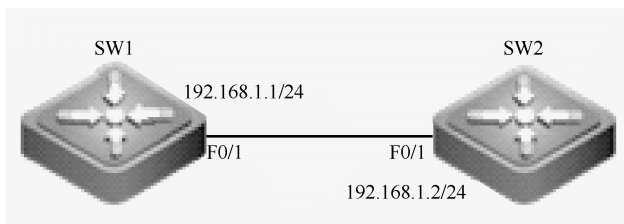


图 3-2-2 接口互连方式

- SW1 的 F0/1 使用路由口，SW2 的 F0/1 使用路由口。
- SW1 使用 SVI，F0/1 为 ACCESS 口，SW2 使用 SVI，F0/1 为 ACCESS 口。
- SW1 使用 SVI，F0/1 为 TRUNK 口，SW2 使用 SVI，F0/1 为 TRUNK 口。

其余情况不再详细介绍。

在校园网中，汇聚交换机上配置 SVI 充当用户的网关。同一个汇聚交换机下的不同接入交换机上的用户就使用三层交换机的直连路由进行通信。汇聚交换机连接核心的接口以及核心交换机上的接口一般建议配置成路由口。

3.2.2 配置三层交换机静态路由技术

三层交换机中静态路由的配置方法与路由器一致，具体命令如下。

```
switch(config)#ip route 目的网段 掩码 下一跳 IP/出接口
```



需要注意的是，配置时如果使用出接口的方式，则应使用三层接口。

也就是说，出接口应当写为路由口或 SVI 口，而不能写为 ACCESS 或 TRUNK 等交换机二层接口。

如图 3-2-3 所示，SW2 有到 192.168.5.0/24 的路由，如果 SW1 要发数据到 192.168.5.0/24，则需要将数据发送给 SW2。

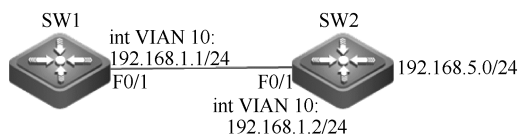


图 3-2-3 三层交换机静态路由

此时，SW1 上配置静态路由为 “ip route 192.168.5.0 255.255.255.0 192.168.1.2”，也可以使用 “ip route 192.168.5.0 255.255.255.0 vlan 10”，出接口不能使用 F0/1 口。

如果三层交换机使用 SVI 配置地址，则数据转发时，查到路由表出接口为 SVI 口，会查询 MAC 地址表并通过下一跳 MAC 找到 SVI 对应的物理接口。

3.2.3 配置三层交换机 RIP 动态路由技术

三层交换机上配置动态路由的方法与路由器一样。

但当使用三层交换机配置 IP 时，如果将该 SVI 对应的网段通告出去，则 RIP 协议报文会从相应 SVI 对应的所有物理接口发送。如果要修改接口的参数，则一般在 SVI 上进行修改。

需要说明的是，如果三层交换机使用 SVI 配置 IP，则路由表中下一跳为 SVI 接口。

配置 RIP 的命令如下。

```
switch(config)# router rip          ! 创建路由进程
switch(config-router)# version {1 | 2} ! 指定版本，默认发送 v1 更新包
switch(config-router)# no auto-summary ! 关闭自动汇总功能，默认是开启的
switch(config-router)# network network-number ! 通告直连网段
```

【综合实训】：配置三层交换机直连路由

网络场景

如图 3-2-4 所示，两台 RG-S5750-28GT-L 设备相互连接，互连接口为 G0/1。要令两台交换机相互通信，需要配置互连地址，交换机 SW1 的地址为 192.168.1.1/24，交换机 SW2 的地址为 192.168.1.2/24。需要根据以下情况将互连地址配置在交换机上。

三层交换机可以使用 no switchport 的方式配置 IP 地址，也可以使用 SVI 地址，而在使用 VLAN 口的地址时，交换机接口可以配置为 ACCESS 或 TRUNK 两种方式。因此设备互连也有多种方式。

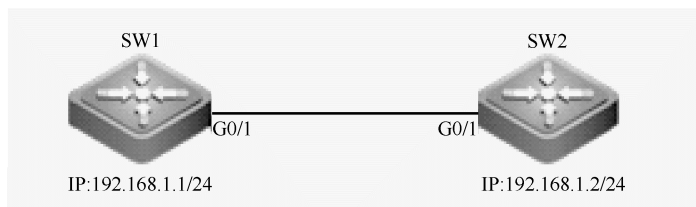


图 3-2-4 交换机直连路由

实施过程

方式一：SW1 的 G0/1 使用 no switchport 接口，SW2 的 G0/1 使用 no switchport 接口。

1. 配置地址

➤ SW1 的配置如下。

```

Ruijie>
Ruijie>en
Ruijie#config t
Ruijie(config)#hostname SW1
SW1(config)#int g 0/1
SW1(config-if-GigabitEthernet 0/1)#no switchport      ! 将接口设为路由口
SW1(config-if-GigabitEthernet 0/1)#ip address 192.168.1.1 255.255.255.0
! 为接口配置 IP 地址
SW1(config-if-GigabitEthernet 0/1)#end
SW1#
  
```

➤ SW2 的配置如下。

```

Ruijie>
Ruijie>en
Ruijie#config t
Ruijie(config)#hostname SW2
SW2(config)#int g 0/1
SW2(config-if-GigabitEthernet 0/1)#no switchport
SW2(config-if-GigabitEthernet 0/1)#ip address 192.168.1.2 255.255.255.0
SW2(config-if-GigabitEthernet 0/1)#end
SW2#
  
```

2. 验证

(1) 在 SW1 和 SW2 上可以互相 Ping 通。

(2) 查看路由表，如图 3-2-5 所示。

```
SW1#show ip route
```

(3) 查看 IP 地址，如图 3-2-6 所示。

```
SW1#show ip int b
```



```
SW1#show ip route

Codes: C - connected, S - static, R - RIP, B - BGP

O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set

C    192.168.1.0/24 is directly connected, GigabitEthernet 0/1

C    192.168.1.1/32 is local host.
```

图 3-2-5 SW1 的路由表

```
SW1#show ip int b

Interface                               IP-Address(Pri)    OK?      Status
GigabitEthernet 0/1                    192.168.1.1/24     YES      UP
```

图 3-2-6 SW1 的地址信息

方式二：SW1 的 G0/1 使用 ACCESS 口在 Interface VLAN 10 上配置 IP，SW2 的 G0/1 使用 ACCESS 口在 Interface VLAN 10 上配置 IP。

1. 配置

➤ SW1 的配置如下：

```
Ruijie>en
Ruijie#config t
Ruijie(config)#hostname SW1
SW1(config)#vlan 10                ! 创建 vlan 10
SW1(config-vlan)#int vlan 10       ! 创建 vlan 10 对应的 SVI
SW1(config-if-VLAN 10)#ip address 192.168.1.1 255.255.255.0 ! 配置 IP 地址
SW1(config-if-VLAN 10)#exit
SW1(config)#int gi 0/1
SW1(config-if-GigabitEthernet 0/1)#switchport access vlan 10
! 物理口和 VLAN 关联
SW1(config-if-GigabitEthernet 0/1)#end
```

➤ SW2 的配置如下。

```
Ruijie#config t
Ruijie(config)#hostname SW2
SW2(config)#vlan 10                ! 创建 vlan 10
SW2(config-vlan)#int vlan 10       ! 创建 vlan 10 对应的 SVI
SW2(config-if-VLAN 10)#ip address 192.168.1.2 255.255.255.0 ! 配置 IP 地址
SW2(config-if-VLAN 10)#exit
SW2(config)#int gi 0/1
SW2(config-if-GigabitEthernet 0/1)#switchport access vlan 10
! 物理口和 VLAN 关联
SW2(config-if-GigabitEthernet 0/1)#end
```

2. 验证

(1) SW1 和 SW2 可以相互 Ping 通。

(2) 查看路由表，如图 3-2-7 所示。

```
SW1#show ip route
```

(3) 查看地址信息，如图 3-2-8 所示。

```
SW1#show ip int b
```

```
SW1#show ip route↵
Codes: C - connected, S - static, R - RIP, B - BGP↵
O - OSPF, IA - OSPF inter area↵
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2↵
E1 - OSPF external type 1, E2 - OSPF external type 2↵
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2↵
ia - IS-IS inter area, * - candidate default↵
Gateway of last resort is no set↵
C    192.168.1.0/24 is directly connected, VLAN 10↵
C    192.168.1.1/32 is local host.  ↵
```

图 3-2-7 SW1 的路由表

```
SW1#show ip int b↵
Interface                IP-Address(Pri)    OK?      Status
VLAN 10                 192.168.1.1/24    YES      UP↵
```

图 3-2-8 SW1 的地址信息

方式三：SW1 的 G0/1 使用 TRUNK 口在 Interface VLAN 10 上配置 IP，SW2 的 G0/1 使用 TRUNK 口在 Interface VLAN 10 上配置 IP。

1. 配置

➤ SW1 的配置如下。

```
Ruijie>en
Ruijie#config t
Ruijie(config)#hostname SW1
SW1(config)#vlan 10
SW1(config-vlan)#exit
SW1(config)#int vlan 10
SW1(config-if-VLAN 10)#ip address 192.168.1.1 255.255.255.0
SW1(config-if-VLAN 10)#exit
SW1(config)#int gi 0/1
SW1(config-if-GigabitEthernet 0/1)#switchport mode trunk
SW1(config-if-GigabitEthernet 0/1)#end
```




SW1#

➤ SW2 的配置如下。

```
Ruijie>en
Ruijie#config t
Ruijie(config)#hostname SW2
SW2(config)#vlan 10
SW2(config-vlan)#exit
SW2(config)#int vlan 10
SW2(config-if-VLAN 10)#ip address 192.168.1.2 255.255.255.0
SW2(config-if-VLAN 10)#exit
SW2(config)#int gi 0/1
SW2(config-if-GigabitEthernet 0/1)#switchport mode trunk
SW2(config-if-GigabitEthernet 0/1)#end
SW2#
```

2. 验证

(1) SW1 和 SW2 可以相互 Ping 通。

(2) 查看路由表，如图 3-2-9 所示。

SW1#show ip route

(3) 查看地址信息，如图 3-2-10 所示。

SW1#show ip int b

从上述过程可以看出，使用 no switchport 时，路由表中直连路由的出口是物理口，地址对应的接口是物理口；而使用 SVI 方式时，路由表中的直连路由的出口是 SVI 口而非物理接口，地址对应的接口是 SVI 口。

```
SW1#show ip route↵
Codes: C - connected, S - static, R - RIP, B - BGP↵
        O - OSPF, IA - OSPF inter area↵
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2↵
        E1 - OSPF external type 1, E2 - OSPF external type 2↵
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2↵
        ia - IS-IS inter area, * - candidate default↵

Gateway of last resort is no set↵

C    192.168.1.0/24 is directly connected, VLAN 10↵
C    192.168.1.1/32 is local host.  ↵
```

图 3-2-9 SW1 的路由表

```
SW1#show ip int b↵

Interface                               IP-Address(Pri)    OK?      Status
VLAN 10                               192.168.1.1/24    YES      UP↵
```

图 3-2-10 SW1 的地址信息

【综合实训】：配置三层交换机静态路由

网络场景

如图 3-2-11 所示，SW1 和 SW2 为三层交换机，PC1 和 PC2 分别连接在 SW1 和 SW2 上，SW1 的 G0/1 口与 PC1 相连，SW1 的 G0/2 和 SW2 的 G0/1 相连，SW2 的 G0/2 与 PC2 相连。PC1 的地址为 192.168.1.1/24，PC2 的地址为 192.168.3.2/24。SW1 的 F0/1 口使用 ACCESS 口，使用 Interface VLAN 10 的地址 192.168.1.2 充当用户网关。

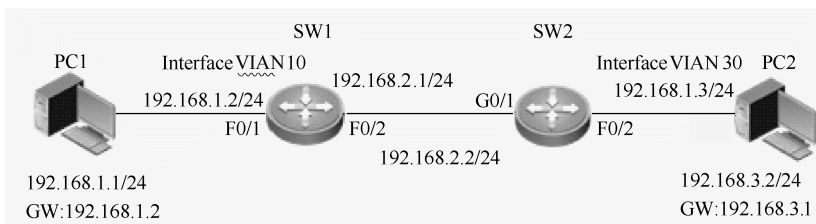


图 3-2-11 静态路由示意图

SW2 的 F0/2 口使用 ACCESS 口，使用 Interface vlan 30 的地址 192.168.3.1 充当用户网关。SW1 的 F0/2 口使用 no switchport，地址为 192.168.2.1/24，SW2 的 F0/1 口使用 no switchport，地址为 192.168.2.2/24。通过配置静态路由使得 PC1 和 PC2 互相进行通信。

实施过程

1. 配置 PC 地址和网关

PC1 的 IP 地址为 192.168.1.1/24，网关为 192.168.1.2。

PC2 的 IP 地址为 192.168.3.2/24，网关为 192.168.3.1。

2. 配置交换机地址

➤ SW1 的配置如下。

```
Ruijie>en
Ruijie#config
Ruijie(config)#hostname SW1
SW1(config)#vlan 10
SW1(config-vlan)#int vlan 10
SW1(config-if-VLAN 10)#ip address 192.168.1.2 255.255.255.0
SW1(config-if-VLAN 10)#exit
SW1(config)#int gi 0/1
SW1(config-if-GigabitEthernet 0/1)#switchport access vlan 10
SW1(config-if-GigabitEthernet 0/1)#exit
SW1(config)#int gi 0/2
SW1(config-if-GigabitEthernet 0/2)#no swi
SW1(config-if-GigabitEthernet 0/2)#ip address 192.168.2.1 255.255.255.0
SW1(config-if-GigabitEthernet 0/2)#exit
```



```
SW1(config)#
```

➤ SW2 的配置如下。

```
Ruijie>en
Ruijie#config
Ruijie(config)#hostname SW2
SW2(config)#vlan 10
SW2(config-vlan)#int vlan 30
SW2(config-if-VLAN 10)#ip address 192.168.3.1 255.255.255.0
SW2(config-if-VLAN 10)#exit
SW2(config)#int gi 0/1
SW2(config-if-GigabitEthernet 0/1)#no swi
SW2(config-if-GigabitEthernet 0/1)#ip address 192.168.2.2 255.255.255.0
SW2(config-if-GigabitEthernet 0/1)#exit
SW2(config)#int gi 0/2
SW2(config-if-GigabitEthernet 0/2)#switchport access vlan 30
SW2(config-if-GigabitEthernet 0/2)#exit
SW2(config)#
```

3. 配置静态路由

➤ SW1 的配置如下。

```
SW1(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2
```

➤ SW2 的配置如下。

```
SW2(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1
```

4. 验证

(1) 两台计算机可以相互 Ping 通。

(2) 查看路由表，如图 3-2-12 所示。

```
SW1#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set

C    192.168.1.0/24 is directly connected, VLAN 10
C    192.168.1.2/32 is local host.
C    192.168.2.0/24 is directly connected, GigabitEthernet 0/2
C    192.168.2.1/32 is local host.
S    192.168.3.0/24 [1/0] via 192.168.2.2
```

图 3-2-12 SW1 的路由表

【综合实训】：配置三层交换机 RIP 动态路由协议

网络场景

如图 3-2-13 所示，SW1 和 SW2 为三层交换机，PC1 和 PC2 分别连在 SW1 和 SW2 上，SW1 的 G0/1 口与 PC1 相连，SW1 的 G0/2 和 SW2 的 G0/1 口相连，SW2 的 G0/2 与 PC2 相连。PC1 的 IP 地址为 192.168.1.1/24，PC2 的 IP 地址为 192.168.3.2/24。SW1 的 F0/1 口使用 ACCESS 口，使用 Interface VLAN 10 的地址 192.168.1.2 充当用户网关。

SW2 的 F0/2 口使用 ACCESS 口，使用 Interface VLAN 30 的地址 192.168.3.1 充当用户网关。SW1 的 F0/2 口使用 no switchport，地址为 192.168.2.1/24；SW2 的 F0/1 口使用 no switchport，地址为 192.168.2.2/24。通过配置 RIP 使得 PC1 和 PC2 能互相通信。

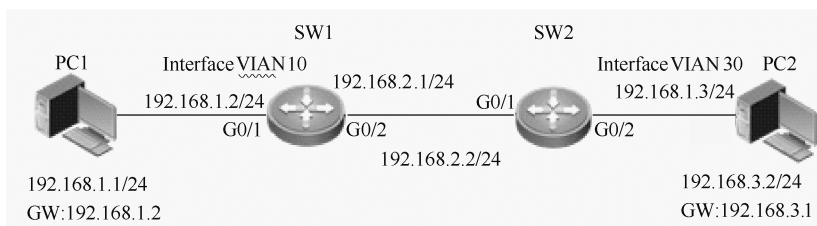


图 3-2-13 动态路由示意图

实施过程

1. 配置 PC 地址和网关

PC1 的 IP 地址为 192.168.1.1/24，网关为 192.168.1.2；

PC2 的 IP 地址为 192.168.3.2/24，网关为 192.168.3.1。

2. 配置交换机地址

➤ SW1 的配置如下。

```
Ruijie>en
Ruijie#config
Ruijie(config)#hostname SW1
SW1(config)#vlan 10
SW1(config-vlan)#int vlan 10
SW1(config-if-VLAN 10)#ip address 192.168.1.2 255.255.255.0
SW1(config-if-VLAN 10)#exit
SW1(config)#int gi 0/1
SW1(config-if-GigabitEthernet 0/1)#switchport access vlan 10
SW1(config-if-GigabitEthernet 0/1)#exit
SW1(config)#int gi 0/2
SW1(config-if-GigabitEthernet 0/2)#no swi
SW1(config-if-GigabitEthernet 0/2)#ip address 192.168.2.1 255.255.255.0
```



```
SW1(config-if-GigabitEthernet 0/2)#exit
```

➤ SW2 的配置如下。

```
Ruijie>en
Ruijie#config
Ruijie(config)#hostname SW2
SW2(config)#vlan 10
SW2(config-vlan)#int vlan 30
SW2(config-if-VLAN 10)#ip address 192.168.3.1 255.255.255.0
SW2(config-if-VLAN 10)#exit
SW2(config)#int gi 0/1
SW2(config-if-GigabitEthernet 0/1)#no swi
SW2(config-if-GigabitEthernet 0/1)#ip address 192.168.2.2 255.255.255.0
SW2(config-if-GigabitEthernet 0/1)#exit
SW2(config)#int gi 0/2
SW2(config-if-GigabitEthernet 0/2)#switchport access vlan 30
SW2(config-if-GigabitEthernet 0/2)#exit
```

3. 配置静态路由

➤ SW1 的配置如下。

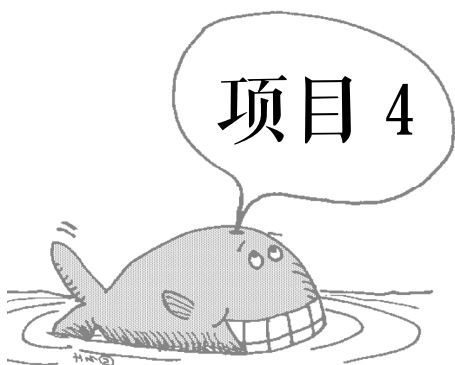
```
SW1(config)#router rip
SW1(config-router)#ver 2
SW1(config-router)#no auto-summary
SW1(config-router)#network 192.168.1.0
SW1(config-router)#network 192.168.2.0
SW1(config-router)#end
```

➤ Switch2 的配置如下。

```
SW2(config)#router rip
SW2(config-router)#ver 2
SW2(config-router)#no auto-summary
SW2(config-router)#network 192.168.1.0
SW2(config-router)#network 192.168.2.0
SW2(config-router)#end
```

4. 验证

- (1) 两台计算机可以相互 Ping 通。
- (2) 查看路由表，验证图略。



配置高级路由技术

任务 1 配置路由器设备链路状态动态路由协议

4.1.1 链路状态动态路由

链路状态路由协议又称为最短路径优先协议，它基于最短路径优先算法。它比距离矢量路由协议复杂得多，但基本功能和配置很简单，甚至算法也容易理解。路由器的链路状态的信息称为链路状态，包括接口的 IP 地址和子网掩码、网络类型、该链路的开销、该链路上的所有相邻路由器。

距离矢量协议和链路状态协议的主要区别如下。

- 生成路由的方式不同。
- 衡量路径优劣的参数不同。

距离矢量协议是平面式的，所有的路由学习完全依靠邻居，交换的是路由表。链路状态路由协议是层次式的，网络中的路由器并不向邻居传递路由表，而是通告给邻居的链路状态。运行该路由协议的路由器不是简单地从相邻的路由器学习路由，而是把路由器分成区域，收集区域的所有路由器的链路状态信息，根据状态信息生成网络拓扑结构，每一个路由器再根据拓扑结构计算出路由。

距离矢量协议选择路径的参数是以跨越路由器的个数为准的。而链路状态协议选择路径的参数是以带宽等链路参数为准的。

距离矢量协议的代表有 RIP 等协议，链路状态协议的代表有 OSPF 等协议。

4.1.2 OSPF 动态路由协议

OSPF 路由协议是一种典型链路状态路由协议，主要维护工作在同一个路由域内网络的连通。在这里，路由域是指一个自治系统（Autonomous System，AS），即是一组通过统一的路



由政策或路由协议，互相交换路由信息的网络。

在自治系统中，所有 OSPF 路由器都维护一个具有相同描述结构的 AS 结构数据库，该数据库中存放路由域中相应的链路状态信息，如图 4-1-1 所示。

每台 OSPF 路由器维护相同自治系统拓扑结构数据库，OSPF 路由器通过这个数据库计算出其 OSPF 路由表。当拓扑发生变化时，OSPF 能迅速重新计算出路径，只产生少量路由协议流量。作为一种经典的链路状态的路由协议，OSPF 将链路状态广播数据包传送给在指定区域内的所有路由器，这一点与距离矢量路由协议不同，运行距离矢量路由协议的路由器将部分或全部的路由表传递给与其相邻的路由器。

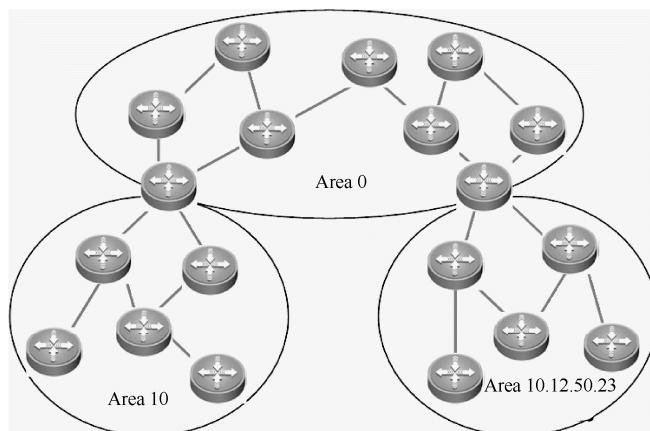


图 4-1-1 具有独立自治系统的网络环境

OSPF 动态路由协议不再采用跳数的概念，而是根据网络中接口的吞吐率、拥塞状况、往返时间、可靠性等实际链路的负载能力，来决定路由选择的代价。同时，选择最短、最优路由作为数据包传输路径，并允许保持到达同一目的地址的多条路由存在，从而平衡网络负荷。此外，OSPF 路由协议还支持不同服务类型的不同代价，从而实现不同 QoS 的路由服务；OSPF 路由器不再交换路由表，而是同步各路由器对网络状态的认识。

OSPF 路由协议是一种链路状态路由协议，为了更好地说明 OSPF 路由协议的基本特征，下面将 OSPF 路由协议与距离矢量路由协议 RIP 进行比较，以便更加清晰地描述 OSPF 路由协议的特点。

1. 网络管理距离不同

在 RIP 路由协议中，其路由的管理距离是 120。而 OSPF 路由协议具有更高的优先级别，其管理距离为 110。

2. 网络范围不同

在 RIP 路由协议中，表示目的网络远近的参数为跳，该参数最大为 15。

在 OSPF 路由协议中，路由表中表示目的网络的参数为路径开销，该参数与网络中链路带宽相关，也就是说，OSPF 路由不受物理跳数限制。因此，OSPF 适用于支持几百台路由器的大型网络。

3. 路由收敛速度不同

路由收敛快慢是衡量路由协议的一个关键指标。

RIP 路由协议周期性地将整个路由表信息广播至网络中，该广播周期为 30s，不仅占用较多网络带宽，还影响网络的更新。

而 OSPF 链路状态路由协议在网络稳定时，网络中路由更新也会减少，并且其更新也不是周期性的，因此 OSPF 在大型网络中能够较快收敛。

4. 构建无环网络

RIP 协议采用 DV 算法，使用该算法的 RIP 协议会产生路由环现象，而且很难清除。

OSPF 采用 SPF 算法，避免了环路产生。SPF 计算结果是一棵树，从根结点到叶子结点是单向不可回复路径，构建了无环网络路径。

5. 安全认证

RIPv1 协议不支持安全认证，修正版本的 RIPv2 增加了部分安全认证功能。

而 OSPF 路由协议支持路由验证，只有通过路由验证，路由器之间才能交换路由信息。OSPF 可以对不同区域定义不同验证方式，提高网络安全性。

6. 路由协议负载分担

RIPv1 协议在传播路由信息时不具有负载分担功能。

而 OSPF 路由协议支持路由负载分担的功能。它支持多条路径开销，可实现相同链路上的负载分担，如果到同一个目的地址有多条路径，而且花费相等，那么可以将多条路径显示在路由表中。

7. 以组播地址发送报文

RIP 使用广播报文传播路由给网络上的所有设备，这种以周期性广播形式的发送会产生一定干扰，同时在一定程度上占用了宝贵的带宽资源。

随着技术发展，出现了以组播地址来发送协议报文的方式。而 OSPF 使用 224.0.0.5 组播地址来发送，只有运行 OSPF 协议的设备才会接收发送来的报文，其他设备不参与接收。

4.1.3 配置路由设备 OSPF 单区域动态路由协议

1. 概述

OSPF 属于内部网关协议，运行在单一自治系统内，是对链路状态路由协议的一种实现，使用最短路径优先算法来计算最短路径树。

OSPF 是 IETF 组织开发的基于链路状态、自治系统内部的动态路由协议。在 IP 网络上，它通过收集和传递自治系统的链路状态来动态发现并传播路由。

OSPF 路由协议适合更广阔范围网络的路由学习，支持 CIDR 及来自外部路由信息选择，同时提供路由选择更新验证，利用 IP 组播发送/接收更新资料。此外，OSPF 协议还支持各种规模的网络，具有快速收敛、支持安全验证、区域划分等特点。

OSPF 支持区域划分，可适应大规模网络。目前 OSPF 在应用中有以下两个版本。



- v2, 适用于 IPv4 环境。
- v3, 扩展支持 IPv6。

2. OSPF 中相关的概念

- 自治系统, 指使用同一种路由协议交换路由信息的一组路由器, 本章中指运行了 OSPF 的一组路由设备的集合。
- 路由 ID (Router-ID), 用于在 AS 中唯一标识一台运行 OSPF 的路由器的 32 位整数, 每个运行 OSPF 的路由器都必须有一个 Router ID。
- 邻居 (Neighbor), 设备启动 OSPF 路由协议后, 便会通过接口向外发送 Hello 报文。收到 Hello 报文的其他启动 OSPF 路由协议的设备会检查报文中所定义的一些参数, 如果双方一致, 则会形成邻居关系。
- 邻接 (Adjacency), 形成邻居关系的双方不一定都能形成邻接关系, 当两台路由设备之间交换路由信息通告, 并在此基础上建立了自己的链路状态数据库之后, 才形成了邻接的关系。

3. OSPF 工作原理

OSPF 简单来说就是两个相邻的路由器通过发送报文的形式成为邻居关系, 邻居再相互发送链路状态信息形成邻接关系, 之后各自根据最短路径算法计算出路由, 放在 OSPF 路由表中, OSPF 路由与其他路由比较后, 最优的会被加入全局路由表。整个过程使用了五种报文、三个阶段、四张表。

(1) 五种报文

- Hello 报文: 建立并维护邻居关系。
- DBD 报文: 发送链路状态头部信息。
- LSR 报文: 把从 DBD 中找出的需要的链路状态头部信息传给邻居, 请求完整信息。
- LSU 报文: 将 LSR 请求的头部信息对应的完整信息发给邻居。
- LSACK: 收到 LSU 报文后确认该报文。

(2) 三个阶段

- 邻居发现: 通过发送 Hello 报文形成邻居关系。
- 路由通告: 邻居间发送链路状态信息形成邻接关系。
- 路由计算: 根据最短路径算法算出路由表。

(3) 四张表

- 邻居表: 主要记录形成邻居关系的路由器。
- 链路状态数据库: 记录链路状态信息。
- OSPF 路由表: 通过链路状态数据库得出。
- 全局路由表: OSPF 路由与其他比较得出。

具体工作过程如图 4-1-2 所示。

(1) 启动进程, 从接口发送 Hello 包。

(2) 收到 Hello 包, 检查参数, 若匹配, 则把 Hello 包中的 Router ID 放入邻居表, 标识为 Init 状态, 并将该 Router ID 添加到 Hello 包 (自己将从该接口发送出去的 Hello 包) 的邻居列表中。

(3) 收到的 Hello 包的邻居列表中含有自己的 Router ID, 则标识为 I-way 状态。

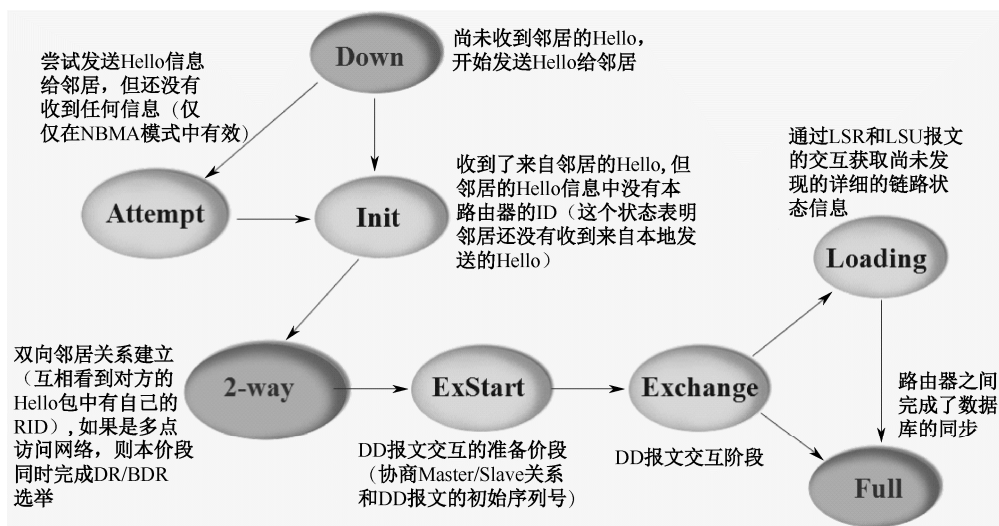


图 4-1-2 OSPF 工作过程

- (4) 点对点链路形成邻接关系，广播、NBMA 网络类型的链路，进行 DR 选举。
- (5) 形成邻接关系，进入 ExStart（准启动）状态，通过 DBD 报文选举主从路由器。
- (6) 主从路由器选举完成，进入 Exchange（交换）状态，通过 DBD 报文描述 LSDB。
- (7) 进入 Loading 状态，对链路状态数据库和收到的 DBD 的 LSA 头部进行比较，发现自己数据库中没有的 LSA 就发送 LSR，向邻居请求该 LSA；邻居收到 LSR 后，回应 LSU；收到邻居发来的 LSU，存储这些 LSA 到自己的链路状态数据库，并发送 LSAck 确认。
- (8) 进入 FULL 状态，LSDB 同步，同一个区域的 OSPF 路由器都拥有相同链路状态数据库。
- (9) 定期发送 Hello 包，维护邻居关系。
- (10) 每台路由器独立进行 SPF 计算，选择最佳路径，放入路由表。

4. OSPF 基本配置

(1) 创建 OSPF 路由进程。

```
Router(config)#router ospf process-id ! process-id 只在本路由器有效
```

(2) 通告直连接口。

```
Router(config-router)#network network wildcard-mask area area-id
! network 为网段, wildcard-mask 为反掩码或者掩码均可, area-id 为区域号
```

(3) 查看及维护类命令。

```
Router# show ip route ! 显示路由表
Router# show ip ospf neighbor detail ! 显示 OSPF 邻居详细信息
Router# show ip ospf database ! 显示拓扑数据库的内容
Router# show ip ospf interface ! 检验已经配置在目的区域中的接口
Router# show ip ospf ! 显示 OSPF 协议信息
Router# clear ip route * ! 清除路由表
Router# debug ip ospf ! 调试 OSPF 协议
```



4.1.4 配置路由设备 OSPF 多区域动态路由协议

1. 多区域 OSPF 背景

如图 4-1-3 所示，单区域 OSPF 主要有以下问题。

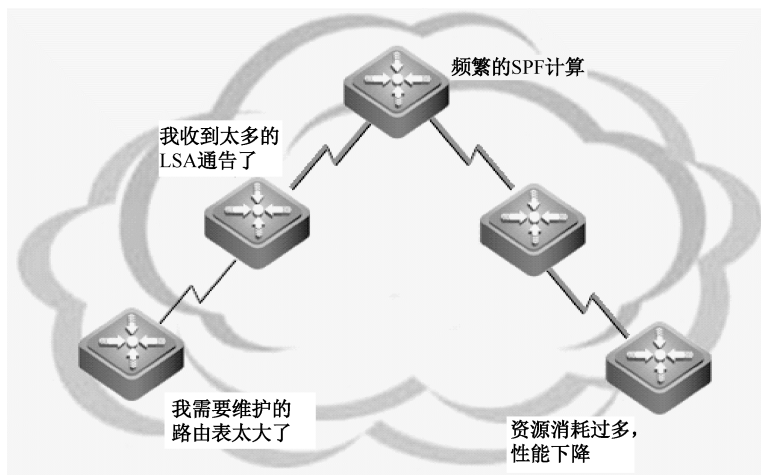


图 4-1-3 单区域 OSPF 示意图

- 同一个区域内所有路由器的 LSDB 完全相同。
- 收到的 LSA 通告太多了。
- 内部链路动荡会引起全网路由器的完全 SPF 计算。
- 区域内路由无法汇总，需要维护的路由表越来越大，资源消耗过多，性能下降，影响数据转发。

如图 4-1-4 所示，多区域 OSPF 可解决以下问题。

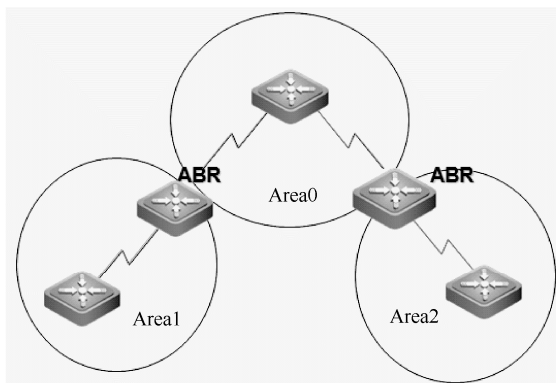


图 4-1-4 多区域 OSPF 示意图

- (1) 把大型网络分隔为多个较小、可管理的单元。
- (2) 网络类型影响邻居关系、毗邻关系的形成及路由计算。
 - 控制 LSA 只在区域内洪泛，有效地把拓扑变化控制在区域内，把拓扑的变化影响限制在本区域。
 - 提高了网络的稳定性和扩展性，有利于组建大规模的网络。
 - 在区域边界可以进行路由汇总，减小了路由表。

2. 多区域 OSPF 工作原理

(1) 多区域 OSPF 区域示意图如图 4-1-5 所示。

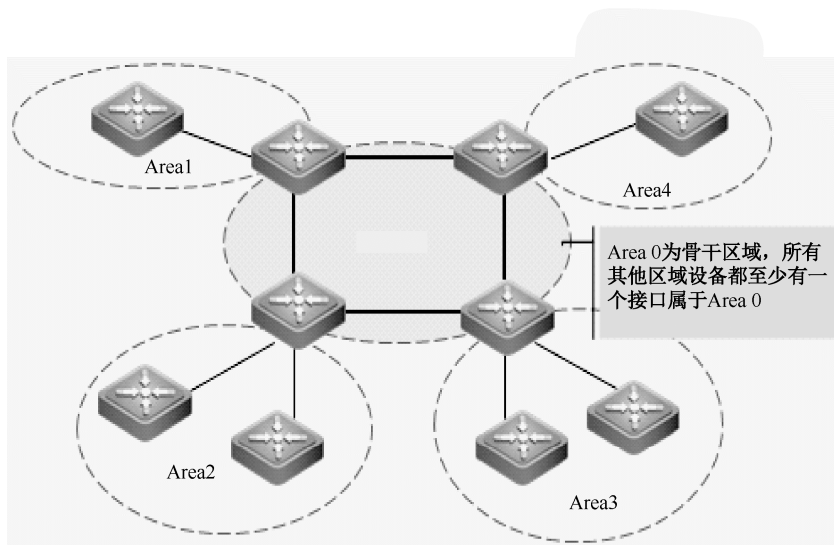


图 4-1-5 多区域 OSPF 区域示意图

Area 0 为骨干区域，骨干区域负责在非骨干区域之间发布由区域边界路由器汇总的路由信息（并非详细的链路状态信息）。

为了避免区域间路由环路，非骨干区域之间不允许直接相互发布区域间路由信息。因此，所有区域边界路由器都至少有一个接口属于 Area 0，即每个区域都必须连接到骨干区域。

多区域 OSPF 具有以下特点。

- LSA 洪泛和链路状态数据库同步只在区域内进行，每个区域都有自己独立的链路状态数据库，SPF 计算独立进行。
- 所有区域必须和骨干区域直接连接，骨干区域必须是连续的。
- 区域边界路由器把区域内的路由转换成区域间路由。
- 形成邻居关系路由器相连的接口必须在同一区域。

(2) OSPF 多区域环境路由器的类型有以下几种。

- 内部路由器（Internal Area Router, IAR），所有接口在同一个 Area 内。同一区域内的所有内部路由器的 LSDB 完全相同。
- 区域边界路由器（Area Border Router, ABR），接口分属于两个或两个以上的区域，并且有一个活动接口属于 Area 0。ABR 为它们所连接的每个区域分别维护单独的 LSDB。区域间路由信息必须通过 ABR 才能进出区域。ABR 是区域路由信息的进出口，也是区域间数据的进出口。
- 主干路由器（Backbone Router, BR），至少有一个接口属于 Area 0 的路由器。
- 自治系统边界路由器（AS Boundary Router, ASBR），通过重发布引入其他路由协议或者其他进程的路由信息。

(3) LSA 类型。OSPF 中常见的 LSA 类型见表 4-1-1。



表 4-1-1 LSA 类型

LSA 类型	由谁产生的	作 用	路由表显示
LSA1	每个 OSPF 路由器	描述区域内部与路由器直连的链路的信息	0
LSA2	DR	描述广播型网络信息	0
LSA3	ABR	描述区域间信息	0IA
LSA4	ABR	描述 ASBR 可达信息	0IA
LSA5	ASBR	描述引入的外部路由	0E2/0E1
LSA7	ASBR	在 NSSA 区域中描述引入的外部路由	0N2/0N1

- 1 类 LSA，路由器 LSA。OSPF 网络中所有路由器都会产生 1 类 LSA，表示路由器自己在本区域内的直连链路信息。该 LSA 仅在本区域内传播。其中，Link ID 和 ADV Router 写的都是该路由器的 Router ID。
- 2 类 LSA，网络 LSA。在广播或者非广播模式下（NBMA）由 DR 生成。该 LSA 仅在本区域内传播。2 类 LSA 表达的意思应该是某区域内，在广播或非广播的网段内选举了 DR，于是 DR 在本区域范围内利用 2 类 LSA 来进行通告。该 LSA 仅在本区域内传播。其中，该 LSA 的 Link ID 就是该 DR 的接口 IP 地址，而 ADV Router 则是 DR 的 Router ID。
- 3 类 LSA，网络汇总 LSA。由区域边界路由器生成，用于将一个区域内的网络通告给 OSPF 中的其他区域。可以认为 3 类 LSA 保存着本区域以外的所有其他区域的网络。
- 4 类 LSA，ASBR 汇总 LSA。4 类 LSA 与 5 类 LSA 是紧密联系在一起的，可以说 4 类 LSA 是由于 5 类 LSA 的存在而产生的。4 类 LSA 由距离本路由器最近的 ABR 生成，即如果路由器想要找到包含了外部路由的那台 ASBR（自治系统边界路由器），则应该到达那台 ABR，这台 ABR 的 Router ID 就写在该 LSA 的 ADV Router 里面，而 LSA 里面的 Link ID 代表的是该 ASBR 的 Router ID。
- 5 类 LSA，外部的 LSA。5 类 LSA 由包含了外部路由的 ASBR 产生，目标是把某外部路由通告给 OSPF 进程的所有区域（特殊区域除外，下面会提到）。5 类 LSA 可以穿越所有区域，即在跨区域通告时，该 LSA 的 Link ID 和 ADV Router 一直保持不变。通俗来说，就像是该 ASBR 对 OSPF 全网络的所有路由器说：“我有这个外部路由，想去的话就来找我吧！”其中，Link ID 代表的是那台 ASBR 所引入的网络，ADV Router 则是该 ASBR 的 Router ID。
- 7 类 LSA，7 类 LSA 是一种由 NSSA 区域中引入了外部路由的路由器生成的 LSA，仅在 NSSA 本区域内传播。由于 NSSA 区域不允许外部的路由进来从而禁止了 5 类 LSA，因此为了能够把自己的外部路由传播出去，使用了 7 类 LSA 来代替 5 类 LSA 的功能。

【综合实训】：配置单区域 OSPF 路由协议

网络场景

如图 4-1-6 所示，某企业有三栋楼，每栋楼都部署了一个路由器，用三台路由器相连，PC1 接在 Router1 上，PC2 接在 Router2 上。PC1 接到 Router1 的 F0/0 口，Router1 的 F0/1 口接到 Router2 的 F0/0 口，Router2 的 F0/1 口接到 Router3 的 F0/0 口，Router3 的 F0/1 口接到 PC2。PC1 的 IP 地址为 192.168.1.1/24，网关为 192.168.1.2。

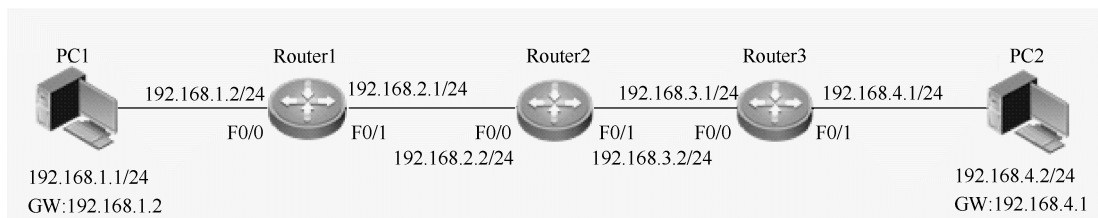


图 4-1-6 单区域 OSPF 示例

Router1 的 F0/0 口的 IP 地址为 192.168.1.2/24，F0/1 口的 IP 地址为 192.168.2.1/24；Router2 的 F0/0 口的 IP 地址为 192.168.2.2/24，F0/1 口的 IP 地址为 192.168.3.1/24；Router3 的 F0/0 口的 IP 地址为 192.168.3.2/24，F0/1 口的 IP 地址为 192.168.4.1/24；PC2 的 IP 地址为 192.168.4.2/24。需要通过配置 OSPF 路由协议使 PC1 和 PC2 通信。

实施过程

1. PC1 和 PC2 的 IP 地址和网关的配置

PC1 的 IP 地址为 192.168.1.1/24，网关为 192.168.1.2。

PC2 的 IP 地址为 192.168.4.2/24，网关为 192.168.4.1。

2. 配置接口 IP 地址

➤ Router1 的配置如下。

```
Ruijie>en
Ruijie#config t
Ruijie(config)#hostname Router1
Router1(config)#int f 0/0
Router1(config-if-FastEthernet 0/0)#ip address 192.168.1.2 255.255.255.0
Router1(config-if-FastEthernet 0/0)#exit
Router1(config)#int f 0/1
Router1(config-if-FastEthernet 0/1)#ip address 192.168.2.1 255.255.255.0
Router1(config-if-FastEthernet 0/1)#exit
Router1(config)#
```

➤ Router2 的配置如下。

```
Ruijie>en
Ruijie#config t
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#hostname Router2
Router2(config)#int f 0/0
Router2(config-if-FastEthernet 0/0)#ip address 192.168.2.2 255.255.255.0
Router2(config-if-FastEthernet 0/0)#exi
Router2(config)#int f 0/1
Router2(config-if-FastEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Router2(config-if-FastEthernet 0/1)#exit
Router2(config)#
```

➤ Router3 的配置如下。

```
Ruijie>en
```



```
Ruijie#con
Ruijie(config)#hostname Router3
Router3(config)#int f 0/0
Router3(config-if-FastEthernet 0/0)#ip address 192.168.3.2 255.255.255.0
Router3(config-if-FastEthernet 0/0)#exit
Router3(config)#int f 0/1
Router3(config-if-FastEthernet 0/1)#ip address 192.168.4.1 255.255.255.0
Router3(config-if-FastEthernet 0/1)#exit
Router3(config)#
```

3. 配置 OSPF

➤ Router1 的配置如下。

```
Router1(config)#router ospf 100      ! 创建 OSPF 协议
Router1(config-router)#network 192.168.1.0 0.0.0.255 area 0  ! 通告直连接口
Router1(config-router)#network 192.168.2.0 0.0.0.255 area 0  ! 通告直连接口
Router1(config-router)#end
```

➤ Router2 的配置如下。

```
Router2(config)#router ospf 100      ! 创建 OSPF 协议
Router2(config-router)#network 192.168.2.0 0.0.0.255 area 0  ! 通告直连接口
Router2(config-router)#network 192.168.3.0 0.0.0.255 area 0  ! 通告直连接口
Router2(config-router)#end
Router2#
```

➤ Router3 的配置如下。

```
Router3(config)#router ospf 100      ! 创建 OSPF 协议
Router3(config-router)#network 192.168.3.0 0.0.0.255 area 0  ! 通告直连接口
Router3(config-router)#network 192.168.4.0 0.0.0.255 area 0  ! 通告直连接口
Router3(config-router)#end
Router3#
```

备注：配置 OSPF 时只需要在通告直连的接口网段后面加反掩码和区域号即可。互连的接口的区域号相同，OSPF 的进程号可以不同。

4. 验证

(1) PC1 和 PC2 之间可以互相 Ping 通。

(2) 查看路由信息。

➤ 查看 OSPF 邻居状态，如图 4-1-7 所示。

```
Router1#show ip ospf neighbor
```

备注：相邻的路由器形成邻居关系时正常情况大部分为 FULL 状态。如果 Area 号不一致，则无法形成邻居关系。

```

router1#show ip ospf neighbor
OSPF process 100, 1 Neighbors, 1 is Full:
Neighbor ID Pri State BFD State Dead Time Address Interface
192.168.3.1 1 Full/BDR - 00:00:35 192.168.2.2 FastEthernet 0/1

router2#show ip ospf neighbor
OSPF process 100, 2 Neighbors, 2 is Full:
Neighbor ID Pri State BFD State Dead Time Address Interface
192.168.2.1 1 Full/DR - 00:00:32 192.168.2.1 FastEthernet 0/0
192.168.4.1 1 Full/BDR - 00:00:33 192.168.3.2 FastEthernet 0/1

router3#show ip ospf neighbor
OSPF process 100, 1 Neighbors, 1 is Full:
Neighbor ID Pri State BFD State Dead Time Address Interface
192.168.3.1 1 Full/DR - 00:00:37 192.168.3.1 FastEthernet 0/0

```

图 4-1-7 OSPF 邻居信息

➤ 查看路由表，如图 4-1-8~图 4-1-10 所示。

```
Router1#show ip route
```

备注：以 O 开头的路由为 OSPF 协议学习到的路由。管理距离为 110，metric 为各链路开销的总和。

```

router1#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
C 192.168.1.0/24 is directly connected, FastEthernet 0/0
C 192.168.1.2/32 is local host.
C 192.168.2.0/24 is directly connected, FastEthernet 0/1
C 192.168.2.1/32 is local host.
O 192.168.3.0/24 [110/2] via 192.168.2.2, 00:16:24, FastEthernet 0/1
O 192.168.4.0/24 [110/3] via 192.168.2.2, 00:13:32, FastEthernet 0/1

```

图 4-1-8 Router1 的路由表

```

router2#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
O 192.168.1.0/24 [110/2] via 192.168.2.1, 00:16:45, FastEthernet 0/0
C 192.168.2.0/24 is directly connected, FastEthernet 0/0
C 192.168.2.2/32 is local host.
C 192.168.3.0/24 is directly connected, FastEthernet 0/1
C 192.168.3.1/32 is local host.
O 192.168.4.0/24 [110/2] via 192.168.3.2, 00:13:50, FastEthernet 0/1

```

图 4-1-9 Router2 的路由表

```

router3#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
O 192.168.1.0/24 [110/3] via 192.168.3.1, 00:14:05, FastEthernet 0/0
O 192.168.2.0/24 [110/2] via 192.168.3.1, 00:14:05, FastEthernet 0/0
C 192.168.3.0/24 is directly connected, FastEthernet 0/0
C 192.168.3.2/32 is local host.
C 192.168.4.0/24 is directly connected, FastEthernet 0/1
C 192.168.4.1/32 is local host.

```

图 4-1-10 Router3 的路由表



【综合实训】：配置多区域 OSPF 路由协议

网络场景

如图 4-1-11 所示，PC1 接到 Router1 的 F0/0 口，Router1 的 F0/1 口接到 Router2 的 F0/0 口，Router2 的 F0/1 口接到 Router3 的 F0/0 口，Router3 的 F0/1 口接到 PC2。PC1 的 IP 地址为 192.168.1.1/24，网关为 192.168.1.2。

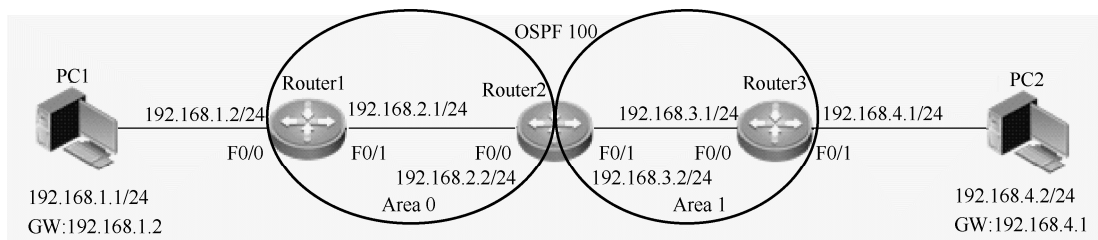


图 4-1-11 多区域 OSPF 示例

Router1 的 F0/0 口的 IP 地址为 192.168.1.2/24，F0/1 口的 IP 地址为 192.168.2.1/24；Router2 的 F0/0 口的 IP 地址为 192.168.2.2/24，F0/1 口的 IP 地址为 192.168.3.1/24；Router3 的 F0/0 口的 IP 地址为 192.168.3.2/24，F0/1 口的 IP 地址为 192.168.4.1/24；PC2 的 IP 地址为 192.168.4.2/24。

需要配置 OSPF 多区域路由协议，其中 Router1 和 Router2 在 Area 0 中，Router2 和 Router3 在 Area 1 中，使 PC1 和 PC2 可以互相通信。

实施过程

1. PC1 和 PC2 的 IP 地址和网关的配置

PC1 的 IP 地址为 192.168.1.1/24，网关为 192.168.1.2。

PC2 的 IP 地址为 192.168.4.2/24，网关为 192.168.4.1。

2. 配置接口 IP 地址

➤ Router1 的配置如下。

```
Ruijie>en
Ruijie#config t
Ruijie(config)#hostname Router1
Router1(config)#int f 0/0
Router1(config-if-FastEthernet 0/0)#ip address 192.168.1.2 255.255.255.0
Router1(config-if-FastEthernet 0/0)#exit
Router1(config)#int f 0/1
```

```
Router1(config-if-FastEthernet 0/1)#ip address 192.168.2.1 255.255.255.0
Router1(config-if-FastEthernet 0/1)#exit
Router1(config)#
```

➤ Router2 的配置如下。

```
Ruijie>en
Ruijie#config t
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#hostname router2
Router2(config)#int f 0/0
Router2(config-if-FastEthernet 0/0)#ip address 192.168.2.2 255.255.255.0
Router2(config-if-FastEthernet 0/0)#exit
Router2(config)#int f 0/1
Router2(config-if-FastEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Router2(config-if-FastEthernet 0/1)#exit
Router2(config)#
```

➤ Router3 的配置如下。

```
Ruijie>en
Ruijie#con
Ruijie(config)#hostname Router3
Router3(config)#int f 0/0
Router3(config-if-FastEthernet 0/0)#ip address 192.168.3.2 255.255.255.0
Router3(config-if-FastEthernet 0/0)#exit
Router3(config)#int f 0/1
Router3(config-if-FastEthernet 0/1)#ip address 192.168.4.1 255.255.255.0
Router3(config-if-FastEthernet 0/1)#exit
Router3(config)#
```

3. 配置 OSPF

➤ Router1 的配置如下。

```
Router1(config)#router ospf 100      ! 创建 OSPF 协议
Router1(config-router)#network 192.168.1.0 0.0.0.255 area 0 ! 通告直连接口
Router1(config-router)#network 192.168.2.0 0.0.0.255 area 0 ! 通告直连接口
Router1(config-router)#end
```

➤ Router2 的配置如下。

```
Router2(config)#router ospf 100      ! 创建 OSPF 协议
Router2(config-router)#network 192.168.2.0 0.0.0.255 area 0 ! 通告直连接口
Router2(config-router)#network 192.168.3.0 0.0.0.255 area 1 ! 通告直连接口
Router2(config-router)#end
Router2#
```

➤ Router3 的配置如下。

```
Router3(config)#router ospf 100      ! 创建 OSPF 协议
Router3(config-router)#network 192.168.3.0 0.0.0.255 area 1 ! 通告直连接口
Router3(config-router)#network 192.168.4.0 0.0.0.255 area 1 ! 通告直连接口
Router3(config-router)#end
Router3#
```



备注：多区域需要有 Area0 且其他 Area 要和 Area0 相连。邻居的 Area 编号要一致且同一个设备可以在多个 Area 中。

4. 验证

(1) PC1 和 PC2 之间可以互相 Ping 通。

(2) 查看路由信息。

➤ 查看 OSPF 邻居状态，如图 4-1-12~图 4-1-14 所示。

Router1#show ip ospf database

备注：对于多区域 OSPF 中，LSA1 和 LSA2 是区域内产生的，LSA3 是区域间产生的。区域内部的路由信息以“O”开头，而 LSA3 学习到的路由以“O IA”开头。

```
router1#show ip ospf database
OSPF Router with ID (192.168.2.1) (Process ID 100)
  Router Link States (Area 0.0.0.0)
    Link ID      ADV Router      Age      Seq#          CkSum  Link count
    192.168.2.1  192.168.2.1    151     0x80000009   0x0a14  2
    192.168.3.1  192.168.3.1    653     0x8000000a   0xc7cc  1
    192.168.4.1  192.168.4.1    1443    0x80000006   0x2ee8  2
  Network Link States (Area 0.0.0.0)
    Link ID      ADV Router      Age      Seq#          CkSum
    192.168.2.1  192.168.2.1    151     0x80000004   0x950f
  Summary Link States (Area 0.0.0.0)
    Link ID      ADV Router      Age      Seq#          CkSum  Route
    192.168.3.0  192.168.3.1    659     0x80000001   0x7b07  192.168.3.0/24
    192.168.4.0  192.168.3.1    585     0x80000001   0x7a06  192.168.4.0/24
```

图 4-1-12 Router1 链路状态数据库

```
router2#show ip ospf database
OSPF Router with ID (192.168.3.1) (Process ID 100)
  Router Link States (Area 0.0.0.0)
    Link ID      ADV Router      Age      Seq#          CkSum  Link count
    192.168.2.1  192.168.2.1    179     0x80000009   0x0a14  2
    192.168.3.1  192.168.3.1    680     0x8000000a   0xc7cc  1
    192.168.4.1  192.168.4.1    1470    0x80000006   0x2ee8  2
  Network Link States (Area 0.0.0.0)
    Link ID      ADV Router      Age      Seq#          CkSum
    192.168.2.1  192.168.2.1    179     0x80000004   0x950f
  Summary Link States (Area 0.0.0.0)
    Link ID      ADV Router      Age      Seq#          CkSum  Route
    192.168.3.0  192.168.3.1    686     0x80000001   0x7b07  192.168.3.0/24
    192.168.4.0  192.168.3.1    612     0x80000001   0x7a06  192.168.4.0/24
  Router Link States (Area 0.0.0.1)
    Link ID      ADV Router      Age      Seq#          CkSum  Link count
    192.168.3.1  192.168.3.1    614     0x80000005   0xe3b3  1
    192.168.4.1  192.168.4.1    608     0x80000006   0x38dd  2
  Network Link States (Area 0.0.0.1)
    Link ID      ADV Router      Age      Seq#          CkSum
    192.168.3.2  192.168.4.1    620     0x80000001   0x8a17
  Summary Link States (Area 0.0.0.1)
    Link ID      ADV Router      Age      Seq#          CkSum  Route
    192.168.1.0  192.168.3.1    686     0x80000001   0x9be7  192.168.1.0/24
```

图 4-1-13 Router2 链路状态数据库

```
router3#show ip ospf database
OSPF Router with ID (192.168.4.1) (Process ID 100)
  Router Link States (Area 0.0.0.1)
    Link ID      ADV Router      Age      Seq#          CkSum  Link count
    192.168.3.1  192.168.3.1    635     0x80000005   0xe3b3  1
    192.168.4.1  192.168.4.1    628     0x80000006   0x38dd  2
  Network Link States (Area 0.0.0.1)
    Link ID      ADV Router      Age      Seq#          CkSum
    192.168.3.2  192.168.4.1    640     0x80000001   0x8a17
  Summary Link States (Area 0.0.0.1)
    Link ID      ADV Router      Age      Seq#          CkSum  Route
    192.168.1.0  192.168.3.1    707     0x80000001   0x9be7  192.168.1.0/24
    192.168.2.0  192.168.3.1    707     0x80000001   0x86fc  192.168.2.0/24
```

图 4-1-14 Router3 链路状态数据库

➤ 查看路由表，如图 4-1-15~图 4-1-17 所示。

```

router1#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
C    192.168.1.0/24 is directly connected, FastEthernet 0/0
C    192.168.1.2/32 is local host.
C    192.168.2.0/24 is directly connected, FastEthernet 0/1
C    192.168.2.1/32 is local host.
O IA 192.168.3.0/24 [110/2] via 192.168.2.2, 00:24:20, FastEthernet 0/1
O IA 192.168.4.0/24 [110/3] via 192.168.2.2, 00:23:11, FastEthernet 0/1

```

图 4-1-15 Router1 的路由信息

```

router2#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
O    192.168.1.0/24 [110/2] via 192.168.2.1, 01:40:13, FastEthernet 0/0
C    192.168.2.0/24 is directly connected, FastEthernet 0/0
C    192.168.2.2/32 is local host.
C    192.168.3.0/24 is directly connected, FastEthernet 0/1
C    192.168.3.1/32 is local host.
O    192.168.4.0/24 [110/2] via 192.168.3.2, 00:23:28, FastEthernet 0/1

```

图 4-1-16 Router2 的路由信息

```

router3#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
O IA 192.168.1.0/24 [110/3] via 192.168.3.1, 00:23:40, FastEthernet 0/0
O IA 192.168.2.0/24 [110/2] via 192.168.3.1, 00:23:40, FastEthernet 0/0
C    192.168.3.0/24 is directly connected, FastEthernet 0/0
C    192.168.3.2/32 is local host.
C    192.168.4.0/24 is directly connected, FastEthernet 0/1
C    192.168.4.1/32 is local host.

```

图 4-1-17 Router3 的路由信息

任务 2 配置路由器路由重发布技术

4.2.1 路由重发布

在大型的网路中，可能使用到多种路由协议。但正常情况下，不同路由协议相互之间不会学习。例如，路由器不会把静态路由通过 OSPF 告诉给邻居。

为了实现多种路由协议的协同工作，路由器可以使用路由重发布技术将其学习到的一种路由协议的路由通过另一种路由协议广播出去，这样网络的所有部分都可以连通了。为了实现重分发，路由器必须同时运行多种路由协议，这样，每种路由协议才可以获取路由表中的



所有或部分其他协议的路由来进行广播。

路由重发布的状况有以下几种。

- 把静态路由重发布到动态路由中。
- 把直连路由重发布到动态路由中。
- 把动态路由协议重发布到另一个动态路由协议中，此时一般使用双向重发布。

不能将动态路由协议重发布到静态路由协议中。

如图 4-2-1 所示，在校园网中，如果内网设备数量较多，则一般使用动态路由协议，目前大部分校园网使用 OSPF 协议。而为了减小出口路由器的负担，在出口设备和核心设备上配置了静态路由。这样对于核心交换机来说，既向出口设备配置了默认路由，又和汇聚交换机运行了 OSPF 等动态协议。核心交换机的路由表中有默认路由和动态路由。

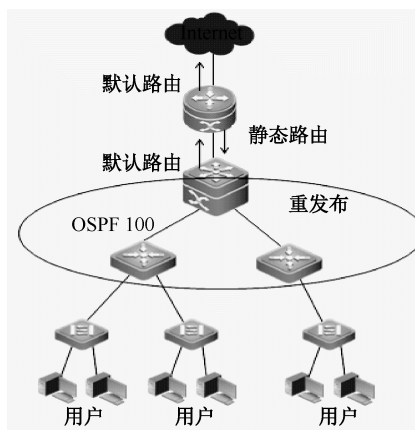


图 4-2-1 校园网路由配置

此时，需要在核心交换机上做重发布，将默认路由重发布到动态路由协议中，否则核心交换机默认不会将默认路由通过动态路由协议告诉给汇聚交换机。因此，汇聚交换机上学习不到默认路由，数据也就无法访问外网。此外，在金融等其他行业网络中，重发布的技术也是很重要的。

4.2.2 使用 RIP 协议的路由重发布

在实施 RIP 时，由于不同的路由协议之间无法相互学习路由，必须实施路由重发布。重发布时可以指定引入的外部路由的跳数，如果不特殊指定，则默认重发布路由在 RIP 中的跳数为 1。

重发布的命令如下。

```
ruijie(config)#router rip
ruijie(config-router)#redistribute connect | static | ospf process-id
[subnets] [metric metric]
```

如果将静态路由重发布到 RIP，则配置“static”参数，其余类似。需要注意以下几点。

- 如果要将子网重发布到 RIP 中，则需要添加 subnets 参数。例如，将路由表中静态路由条目 172.16.10.0/24 重发布到 RIP 中，由于 172.16.10.0/24 是子网，因此重发布时需要配置 subnets 命令。
- 默认重发布在 RIP 中的路由的 metric 为 1，如果需要修改，则添加 metric 参数修改 metric 值。
- 如果要将默认路由通过 RIP 发给其他路由器，则需要使用以下命令。

```
ruijie(config-router)#default-information origin
```

4.2.3 使用 OSPF 协议的路由重发布

在 OSPF 协议中重发布可以将其他路由协议或 OSPF 协议加到该 OSPF 进程中。OSPF 使用 5 类 LSA 或在 NSSA、totally NSSA 等特殊区域中使用 7 类 LSA 来转发该路由。在路由表中用“OE2、OE1、ON2、ON1”表示。

OSPF 路由重发布配置在边界路由器上，通过重发布引入其他路由协议或者其他进程的路由，该路由器网络中的用户称之为 ASBR。在 ASBR 进行重发布后，ASBR 会发送 5 类或 7 类的 LSA，并发送该路由信息。

重发布直连路由、静态路由、RIP、其他 OSPF 等动态路由，配置命令如下。

```
Ruijie(config)# router ospf process-id
Ruijie(config-router)#redistribute 协议进程号 [subnets] [metric metric]
[metric-type type]
```

重发布有以下特点。

- 重发布默认类型是 OE2，使用“metric-type 1”参数可以强制指定为 OE1。
- 如果需要重发布子网，则需要加“subnets”参数。
- 默认在 OSPF 中重发布的路由的 metric 为 20，如果需要修改，则可使用“metric metric”进行修改。
- 如果要修改 metric 的类型，则可使用“metric-type type”进行修改。默认使用 OE2 类型。OE2 和 OE1 的区别主要是 OE2 计算 metric 只计算外部开销，而 OE1 是计算内部开销加外部开销。也就是说，OE2 的路由条目在 OSPF 网络中传送时 metric 不变，而 OE1 路由条目在 OSPF 网络中传送时 metric 会增加。
- 默认路由以特殊的命令引入。

引入默认路由的命令为：

```
Ruijie(config)#router ospf process-id
Ruijie(config-router)#default-information originate [always]
```

引入的默认路由 metric 默认为 1，可以使用“metric metric”命令修改。

默认情况下，只有当路由表有默认路由时才会引入这个默认路由；使用“always”时，路由表中无论有无默认路由都重发布。

【综合实训】：RIP 中路由重发布

网络场景

如图 4-2-2 所示，顶新一公司有两栋楼、顶新二公司有一栋楼，Router1 和 Router2 为顶新一公司的两台路由器，Router3 为顶新二公司的路由器。PC1 接到 Router1 的 F0/0 口，Router1 的 F0/1 口接到 Router2 的 F0/0 口，Router2 的 F0/1 口接到 Router3 的 F0/0 口，Router3 的 F0/1 口接到 PC2。PC1 的 IP 地址为 192.168.1.1/24，网关为 192.168.1.2。

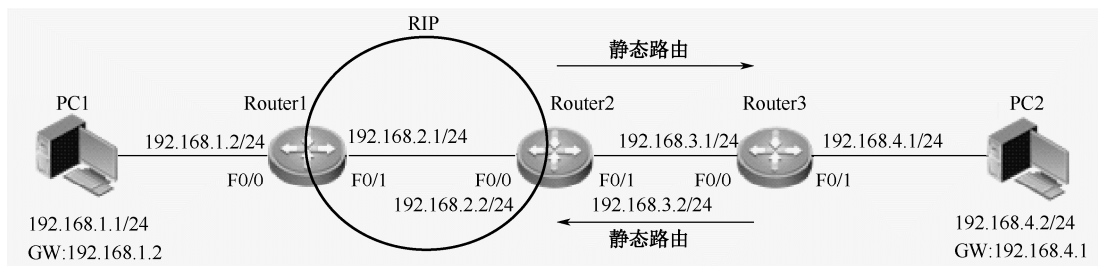


图 4-2-2 RIP 协议路由重发布

Router1 的 F0/0 口的 IP 地址为 192.168.1.2/24，F0/1 口的 IP 地址为 192.168.2.1/24；Router2 的 F0/0 口的 IP 地址为 192.168.2.2/24，F0/1 口的 IP 地址为 192.168.3.1/24；Router3 的 F0/0 口的 IP 地址为 192.168.3.2/24，F0/1 口的 IP 地址为 192.168.4.1/24；PC2 的 IP 地址为 192.168.4.2/24。

其中，顶新一公司使用 RIP 协议，顶新一公司和二公司使用静态路由协议，使 PC1 和 PC2 可以通信。

实施过程

1. PC1 和 PC2 的 IP 地址和网关的配置

PC1 的 IP 地址为 192.168.1.1/24，网关为 192.168.1.2。

PC2 的 IP 地址为 192.168.4.2/24，网关为 192.168.4.1。

2. 配置接口 IP 地址

➤ Router1 的配置如下。

```
Ruijie>en
Ruijie#config t
Ruijie(config)#hostname Router1
Router1(config)#int f 0/0
Router1(config-if-FastEthernet 0/0)#ip address 192.168.1.2 255.255.255.0
Router1(config-if-FastEthernet 0/0)#exit
Router1(config)#int f 0/1
Router1(config-if-FastEthernet 0/1)#ip address 192.168.2.1 255.255.255.0
Router1(config-if-FastEthernet 0/1)#exit
Router1(config)#
```

➤ Router2 的配置如下。

```
Ruijie>en
Ruijie#config t
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#hostname Router2
Router2(config)#int f 0/0
Router2(config-if-FastEthernet 0/0)#ip address 192.168.2.2 255.255.255.0
Router2(config-if-FastEthernet 0/0)#exit
Router2(config)#int f 0/1
```

```
Router2(config-if-FastEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Router2(config-if-FastEthernet 0/1)#exit
Router2(config)#
```

➤ Router3 的配置如下。

```
Ruijie>en
Ruijie#con
Ruijie(config)#hostname Router3
Router3(config)#int f 0/0
Router3(config-if-FastEthernet 0/0)#ip address 192.168.3.2 255.255.255.0
Router3(config-if-FastEthernet 0/0)#exit
Router3(config)#int f 0/1
Router3(config-if-FastEthernet 0/1)#ip address 192.168.4.1 255.255.255.0
Router3(config-if-FastEthernet 0/1)#exit
Router3(config)#
```

3. 配置 RIP 路由协议

➤ Router1 的配置如下。

```
Router1(config)#router rip
Router1(config-router)#version 2
Router1(config-router)#no auto-summary
Router1(config-router)#network 192.168.2.0
Router1(config-router)#end
Router1#
```

备注：Router1 不通告 192.168.1.0/24 网段，该网段进行重发布。

➤ Router2 的配置如下。

```
Router2(config)#rout rip
Router2(config-router)#version 2
Router2(config-router)#no auto-summary
Router2(config-router)#network 192.168.2.0
Router2(config-router)#network 192.168.3.0
Router2(config-router)#exit
```

4. 配置静态路由

➤ Router2 的配置如下。

```
Router2(config)#ip route 192.168.4.0 255.255.255.0 192.168.3.2
```

➤ Router3 的配置如下。

```
Router3(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1
Router3(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.1
```

备注：可以在 Router3 上进行汇总路由。



5. 在 RIP 中进行重发布

➤ Router1 重发布直连路由。

```
Router1(config)#router rip
Router1(config-router)#redistribute connected
```

➤ Router2 重发布静态路由。

```
Router2(config)#router rip
Router2(config-router)#redistribute static
```

备注：重发布时可以修改 metric 值。

6. 验证

(1) PC1 和 PC2 可以互相 Ping 通。

(2) 查看路由表信息，如图 4-2-3 和图 4-2-4 所示。

```
router1#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
C    192.168.1.0/24 is directly connected, FastEthernet 0/0
C    192.168.1.2/32 is local host.
C    192.168.2.0/24 is directly connected, FastEthernet 0/1
C    192.168.2.1/32 is local host.
R    192.168.3.0/24 [120/1] via 192.168.2.2, 00:56:46, FastEthernet 0/1
R    192.168.4.0/24 [120/1] via 192.168.2.2, 00:01:27, FastEthernet 0/1
```

图 4-2-3 Router1 的路由信息

```
router2#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
R    192.168.1.0/24 [120/1] via 192.168.2.1, 00:02:41, FastEthernet 0/0
C    192.168.2.0/24 is directly connected, FastEthernet 0/0
C    192.168.2.2/32 is local host.
C    192.168.3.0/24 is directly connected, FastEthernet 0/1
C    192.168.3.1/32 is local host.
S    192.168.4.0/24 [1/0] via 192.168.3.2
```

图 4-2-4 Router2 的路由信息

如果此时 Router3 上添加了多个网段，则在 Router2 上配置一条默认路由指向 Router3。

➤ Router2 的配置如下。

```
Router2(config)#ip route 0.0.0.0 0.0.0.0 192.168.3.2 ! 配置默认路由
Router2(config)#router rip
Router2(config-router)#default-information originate ! 重发布默认路由协议
Router2(config-router)#end
```

查看 Router1 和 Router2 的路由表。Router1 和 Router2 的路由信息如图 4-2-5 和图 4-2-6 所示。

```

router1#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
Gateway of last resort is 192.168.2.2 to network 0.0.0.0
R* 0.0.0.0/0 [120/1] via 192.168.2.2, 00:02:23, FastEthernet 0/1
C 192.168.1.0/24 is directly connected, FastEthernet 0/0
C 192.168.1.2/32 is local host.
C 192.168.2.0/24 is directly connected, FastEthernet 0/1
C 192.168.2.1/32 is local host.
R 192.168.3.0/24 [120/1] via 192.168.2.2, 01:06:47, FastEthernet 0/1
R 192.168.4.0/24 [120/1] via 192.168.2.2, 00:11:28, FastEthernet 0/1

```

图 4-2-5 Router1 的路由信息

```

router2#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
Gateway of last resort is 192.168.3.2 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 192.168.3.2
R 192.168.1.0/24 [120/1] via 192.168.2.1, 00:13:11, FastEthernet 0/0
C 192.168.2.0/24 is directly connected, FastEthernet 0/0
C 192.168.2.2/32 is local host.
C 192.168.3.0/24 is directly connected, FastEthernet 0/1
C 192.168.3.1/32 is local host.
S 192.168.4.0/24 [1/0] via 192.168.3.2

```

图 4-2-6 Router2 的路由信息

【综合实训】：OSPF 中的路由重发布

网络场景

如图 4-2-7 所示，顶新一公司有两栋楼，顶新二公司有一栋楼，Router1 和 Router2 为顶新一公司的两台路由器，Router3 为顶新二公司的路由器。PC1 接到 Router1 的 F0/0 口，Router1 的 F0/1 口接到 Router2 的 F0/0 口，Router2 的 F0/1 口接到 Router3 的 F0/0 口，Router3 的 F0/1 口接到 PC2。PC1 的 IP 地址为 192.168.1.1/24，网关为 192.168.1.2。

Router1 的 F0/0 口的 IP 地址为 192.168.1.2/24，F0/1 口的 IP 地址为 192.168.2.1/24；Router2 的 F0/0 口的 IP 地址为 192.168.2.2/24，F0/1 口的 IP 地址为 192.168.3.1/24；Router3 的 F0/0 口的 IP 地址为 192.168.3.2/24，F0/1 口的 IP 地址为 192.168.4.1/24；PC2 的 IP 地址为 192.168.4.2/24。

顶新一公司使用 OSPF 协议，顶新一公司和二公司使用静态路由协议，使 PC1 和 PC2 可以互相通信。

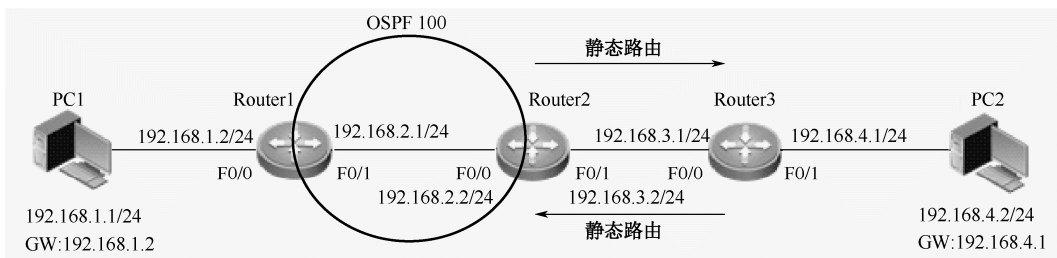


图 4-2-7 OSPF 重发布示意图

实施过程

1. PC1 和 PC2 的 IP 地址和网关的配置

PC1 的 IP 地址为 192.168.1.1/24，网关为 192.168.1.2。

PC2 的 IP 地址为 192.168.4.2/24，网关为 192.168.4.1。

2. 配置接口 IP 地址

➤ Router1 的配置如下。

```
Ruijie>en
Ruijie#config t
Ruijie(config)#hostname Router1
Router1(config)#int f 0/0
Router1(config-if-FastEthernet 0/0)#ip address 192.168.1.2 255.255.255.0
Router1(config-if-FastEthernet 0/0)#exit
Router1(config)#int f 0/1
Router1(config-if-FastEthernet 0/1)#ip address 192.168.2.1 255.255.255.0
Router1(config-if-FastEthernet 0/1)#exit
Router1(config)#
```

➤ Router2 的配置如下。

```
Ruijie>en
Ruijie#config t
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#hostname Router2
Router2(config)#int f 0/0
Router2(config-if-FastEthernet 0/0)#ip address 192.168.2.2 255.255.255.0
Router2(config-if-FastEthernet 0/0)#exit
Router2(config)#int f 0/1
Router2(config-if-FastEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Router2(config-if-FastEthernet 0/1)#exit
Router2(config)#
```

➤ Router3 的配置如下。

```
Ruijie>en
Ruijie#con
Ruijie(config)#hostname Router3
Router3(config)#int f 0/0
```

```
Router3(config-if-FastEthernet 0/0)#ip address 192.168.3.2 255.255.255.0
Router3(config-if-FastEthernet 0/0)#exit
Router3(config)#int f 0/1
Router3(config-if-FastEthernet 0/1)#ip address 192.168.4.1 255.255.255.0
Router3(config-if-FastEthernet 0/1)#exit
```

3. 配置 OSPF 路由协议

➤ Router1 的配置如下。

```
Router1(config)#router ospf 100
Router1(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router1(config-router)#exit
```

备注：Router1 不通告 192.168.1.0/24 网段，该网段进行重发布。

➤ Router2 的配置如下。

```
Router2(config)#router ospf 100
Router2(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router2(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router2(config-router)#exit
```

4. 配置静态路由

➤ Router2 的配置如下。

```
Router2(config)#ip route 192.168.4.0 255.255.255.0 192.168.3.2
```

➤ Router3 的配置如下。

```
Router3(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1
Router3(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.1
```

备注：可以在 Router3 上进行汇总路由。

5. 在 RIP 中进行重发布

➤ Router1 重发布直连路由。

```
Router1(config)#router ospf 100
Router1(config-router)#redistribute connect
```

➤ Router2 重发布静态路由。

```
Router2(config)#router ospf 100
Router2(config-router)#redistribute static metric 5
% Only classful networks will be redistributed
Router2(config-router)#end
Router2#
```

备注：重发布时将 metric 修改为 5，重发布子网需要加“subnets”参数。

6. 验证

PC1 和 PC2 可以 Ping 通。

7. 重发布默认路由

在 Router2 上配置默认路由指向 Router3，并将该默认路由重发布到 OSPF 中。

```
Router2(config)#ip route 0.0.0.0 0.0.0.0 192.168.3.2 ! 配置默认路由
```



```
Router2(config)#router ospf 100
Router2(config-router)#default-information originate ! 将默认路由加入 OSPF 协议
Router2(config-router)#end
Router2#
```

8. 查看路由器链路状态信息

路由器链路状态信息如图 4-2-8 和图 4-2-9 所示。

```
router1#show ip ospf database
OSPF Router with ID (192.168.2.1) (Process ID 100)
Router Link States (Area 0.0.0.0)
Link ID      ADV Router   Age  Seq#       CkSum  Link count
192.168.2.1  192.168.2.1  623  0x80000004 0xe4b6 1
192.168.3.1  192.168.3.1  932  0x80000007 0x23f4 2
Network Link States (Area 0.0.0.0)
Link ID      ADV Router   Age  Seq#       CkSum
192.168.2.2  192.168.3.1  1084 0x80000001 0x861f
AS External Link States
Link ID      ADV Router   Age  Seq#       CkSum  Route                               Tag
0.0.0.0      192.168.3.1  160  0x80000001 0x4849  E2 0.0.0.0/0                      100
192.168.1.0  192.168.2.1  622  0x80000001 0xce19  E2 192.168.1.0/24                0
192.168.4.0  192.168.3.1  931  0x80000001 0x8301  E2 192.168.4.0/24                0
```

图 4-2-8 Router1 的链路状态信息

```
router2#show ip ospf database
OSPF Router with ID (192.168.3.1) (Process ID 100)
Router Link States (Area 0.0.0.0)
Link ID      ADV Router   Age  Seq#       CkSum  Link count
192.168.2.1  192.168.2.1  641  0x80000004 0xe4b6 1
192.168.3.1  192.168.3.1  948  0x80000007 0x23f4 2
Network Link States (Area 0.0.0.0)
Link ID      ADV Router   Age  Seq#       CkSum
192.168.2.2  192.168.3.1  1100 0x80000001 0x861f
AS External Link States
Link ID      ADV Router   Age  Seq#       CkSum  Route                               Tag
0.0.0.0      192.168.3.1  176  0x80000001 0x4849  E2 0.0.0.0/0                      100
192.168.1.0  192.168.2.1  640  0x80000001 0xce19  E2 192.168.1.0/24                0
192.168.4.0  192.168.3.1  947  0x80000001 0x8301  E2 192.168.4.0/24                0
```

图 4-2-9 Router2 的链路状态信息

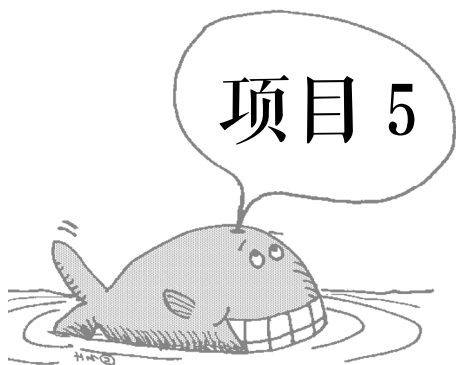
9. 查看路由信息

Router1 和 Router2 的路由信息如图 4-2-10 所示。

```
router1#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default
Gateway of last resort is 192.168.2.2 to network 0.0.0.0
O*E2 0.0.0.0/0 [110/1] via 192.168.2.2, 00:06:49, FastEthernet 0/1
C 192.168.1.0/24 is directly connected, FastEthernet 0/0
C 192.168.1.2/32 is local host.
C 192.168.2.0/24 is directly connected, FastEthernet 0/1
C 192.168.2.1/32 is local host.
O 192.168.3.0/24 [110/2] via 192.168.2.2, 00:22:02, FastEthernet 0/1
O E2 192.168.4.0/24 [110/5] via 192.168.2.2, 00:19:41, FastEthernet 0/1

router2#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default
Gateway of last resort is 192.168.3.2 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 192.168.3.2
O E2 192.168.1.0/24 [110/20] via 192.168.2.1, 00:14:44, FastEthernet 0/0
C 192.168.2.0/24 is directly connected, FastEthernet 0/0
C 192.168.2.2/32 is local host.
C 192.168.3.0/24 is directly connected, FastEthernet 0/1
C 192.168.3.1/32 is local host.
S 192.168.4.0/24 [1/0] via 192.168.3.2
```

图 4-2-10 Router1 和 Router2 的路由信息



配置路由器接入广域网

任务 1 配置路由器广域网链路

5.1.1 广域网链路

广域网 (Wide Area Network, WAN) 通常跨接很大的物理范围, 所覆盖的范围从几十千米到几千千米, 它能连接多个城市或国家, 或横跨几个洲并能提供远距离通信, 形成国际性的远程网络。

局域网只能在一个相对较短的距离内实现, 当主机之间的距离较远时 (如相隔几十或几百千米, 甚至几千千米), 局域网显然无法完成主机之间的通信任务。这时就需要另一种结构的网络, 即广域网。广域网的地理覆盖范围可以从数千米到数千千米, 可以连接若干个城市、地区, 甚至跨越国界而成为遍及全球的一种计算机网络。广域网将地理上相隔很远的局域网互连起来。

由于广域网的造价较高, 一般都是由国家或较大的电信公司出资建造的。广域网是互联网的核心部分, 其任务是通过长距离运送主机所发送的数据。连接广域网各结点交换机的链路都是高速链路, 其距离可以是几千千米的光缆线路, 也可以是几万千米的点对点卫星链路。需要澄清的一个概念是广域网不等于互联网。在互联网中, 为不同类型、协议的网络“互联”才是它的主要特征。

广域网由一些结点交换机及连接这些交换机的链路组成。结点交换机的任务是将分组存储转发, 结点之间都是点到点连接的, 但为了提高网络的可靠性, 一个结点交换机往往与多个结点交换机相连。受经济条件的限制, 广域网都不使用局域网, 普遍采用多点接入技术。从层次上考虑, 广域网和局域网的区别很大, 因为局域网使用的协议主要在数据链路层, 而广域网使用的协议在网络层。



广域网目前应用于大部分行业。在教育行业中主要应用于出口链路。金融行业主要应用于各级分行的互连，如图 5-1-1 所示。政府行业主要应用于各级部门的互连。

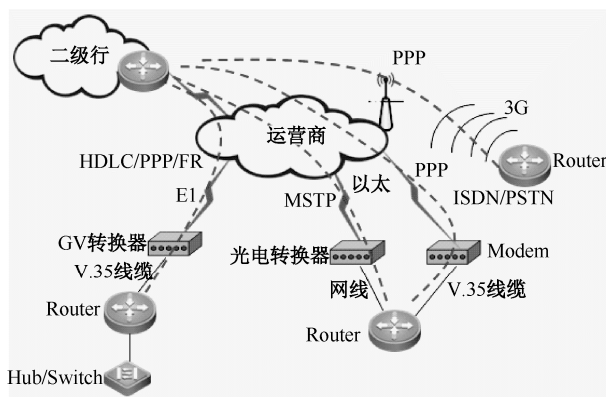


图 5-1-1 广域网链路结构

广域网类型可分为专线、电路交换、分组交换、VPN 等类型。

1. 专线

所谓的专线是由 ISP 为企业远程结点之间的通信提供点到点专有线路连接，为专用逻辑连接，永久在线，支持多种介质与速率，如图 5-1-2 所示。

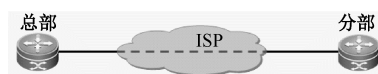


图 5-1-2 专线示意图

典型的专线技术有 DDN、E1、POS、MSTP 等。

2. 电路交换

电路交换是广域网所使用的一种交换方式。可以通过运营商网络为每一次会话过程建立、维持和终止一条专用的物理电路。电路交换也可以提供数据报和数据流两种传送方式。电路交换在电信运营商的网络中被广泛使用，其操作过程与普通的电话拨叫过程非常相似。综合业务数字网（ISDN）就是一种采用电路交换技术的广域网技术。

电路交换是 ISP 为企业远程结点间通信提供的临时数据传输通道，其操作特性类似电话拨号技术，即逻辑连接，按需拨号。传输介质主要为电话线，也可以为光纤。其带宽主要为 56kb/s, 64kb/s, 128kb/s, 2Mkb/s 等，其稳定性较差，配置与维护较复杂。

典型的电路交换技术有 PSTN 模拟拨号和 ISDN 数字拨号等。

3. 分组交换

分组交换是由 ISP 为企业多个远程结点间通信提供的一种共享物理链路的 WAN 技术。通信双方从 ISP 获取 VC 以建立逻辑连接，称为虚电路，一条物理链路上可以包含多条 VC。可根据数据帧的地址来进行路径的选择、共享技术，其费用低，安全性较差，配置复杂。

VC 是按照需求动态建立的，当数据传送结束时，电路将会被自动终止。VC 上的通信过程包括 3 个阶段，即电路创建、数据传输和电路终止。电路创建阶段主要在通信双方设备之间建立起虚拟电路；数据传输阶段通过虚拟电路在设备之间传送数据；电路终止阶段则是撤销在通信设备之间已经建立起来的虚拟电路。SVC 主要适用于非经常性的数据传送网络，这

是因为在电路创建和终止阶段 SVC 需要占用更多的网络带宽，但相对于永久性虚拟电路来说，SVC 的成本较低。

典型的分组交换技术有 FR、ATM、X.25 等。

4. 虚拟专用网络

虚拟专用网络（Virtual Private Network，VPN）指的是本地 LAN 和远程 LAN 通过宽带拨号或固定 IP 获取互联网络的访问，在两者之间建立二层或三层隧道穿越互联网络。其主要用于穿越公网，提供数据加密、数据包完整性检验、身份认证等功能。VPN 安全、经济，接入方便。VPN 的典型类型有 L2TP VPN、IPSec VPN、SSL VPN、MPLS VPN 等。

5.1.2 配置路由器设备的 PPP 协议

点对点链路提供的是一条预先建立的从客户端经过运营商网络到达远端目标网络的广域网通信路径。一条点对点链路就是一条租用的专线，可以在数据收发双方之间建立起永久性的固定连接。网络运营商负责点对点链路的维护和管理。

点对点链路可以提供两种数据传送方式：一种是数据报传送方式，该方式主要是将数据分割成一个个小的数据帧进行传送，其中每一个数据帧都带有自己的地址信息，都需要进行地址校验；另外一种方式是数据流传送方式，该方式与数据报传送方式不同，用数据流取代一个个的数据帧作为数据发送单位，整个流数据具有一个地址信息，只需要进行一次地址验证即可。如图 5-1-3 所示为一个典型的跨越广域网的点对点链路。



图 5-1-3 广域网点对点链路

1. 概述

点到点协议（Point-to-Point Protocol，PPP）是为在同等单元之间传输数据包这样的简单链路设计的链路层协议。这种链路提供全双工操作，并按照顺序传递数据包。设计目的主要是通过拨号或专线方式建立点对点连接并发送数据，使其成为各种主机、交换机和路由器之间简单连接的一种共通的解决方案。

PPP 支持差错检测，支持各种协议，在连接时 IP 地址可复制，具有身份验证功能，可以以各种方式压缩数据、支持动态地址协商、支持多链路捆绑等。这些丰富的选项增强了 PPP 的功能。同时，不论是异步拨号线路还是路由器之间的同步链路均可使用。PPP 不仅适用于拨号用户，还适用于租用的路由器对路由器线路。

PPP 协议是目前使用最广泛的广域网协议，这是因为它具有以下特性。

- 能够控制数据链路的建立。
- 能够对 IP 地址进行分配和使用。
- 允许同时采用多种网络层协议。
- 能够配置和测试数据链路。
- 能够进行错误检测。



- 有协商选项，能够对网络层的地址和数据压缩等进行协商。

2. PPP 协商过程

典型的 PPP 链路协商过程分为以下三个阶段。

- 链路建立阶段。
- 认证阶段（可选）。
- 网络协商阶段。

PPP 的链路协商过程如图 5-1-4 所示。

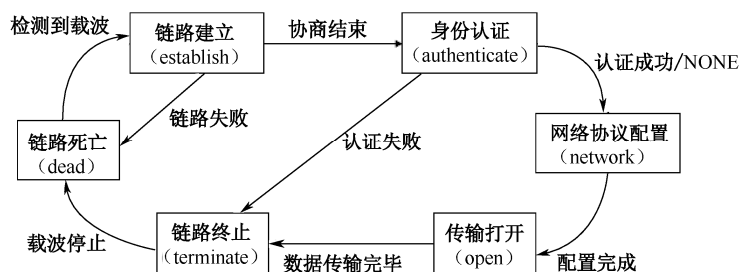


图 5-1-4 PPP 的链路协商过程

PPP 的协商过程主要经过以下五个状态。

- **链路死亡状态 (dead)**。链路一定开始和结束于这个状态。当外部事件（如载波侦听或网络管理员设定）指出物理层已经准备就绪时，PPP 将进入链路建立阶段。
- **链路建立状态 (establish)**。在这个状态下，PPP 通过发送和接收链路配置报文（Configuration），协商具体的参数选项，当收到并发送 Configurations ACK 后，该状态结束，即打开链路。如果线路中断或者配置失效，则将返回链路死亡状态。
- **认证状态 (authenticate)**。在这个状态下协商具体的认证参数，如是否认证、进行什么认证、认证参数交换等，当认证通过或不需认证时开始网络层协议的协商，进入网络层协议配置状态，否则链路终止，最后回到链路死亡阶段。
- **网络层协议配置状态 (network)**。LCP 协商成功将进入 NCP 的协商阶段，在这个阶段中将进行网络层协议的协商，每一种网络层协议（如 IP、IPX 或 AppleTalk）需要单独建立和配置一个 NCP，如果任一 NCP 协商不成功，则随时关闭该 NCP。NCP 协商通过后将可以进行网络报文的通信。如果不成功，则关闭链路并进入链路终止状态，最后返回初始的链路死亡状态。
- **链路终止状态 (terminate)**。因为链路失效、认证失败、链路质量状态失败、链路空闲时间超时以及管理员关闭链路等原因，可随时进入链路终止状态。PPP 协议会在发送 Terminate-Request 并接收到 Terminate-ACK 以后进入该状态。

3. 配置命令

路由器大部分广域网接口默认使用 HDLC 协议，需使用 PPP 协议时，要在两个路由器上手工指定接口类型。基本配置命令如下。

```
ruijie(config)#interface serial interface      ! 进入路由器广域网接口
ruijie(config-if-Serial 0/0)#encapsulation ppp ! 配置接口协议为 PPP 协议
```

【综合实训】：配置路由器 PPP 协议

网络场景

如图 5-1-5 所示，路由器 RA 和 RB 通过 S0/0 相连，要配置点到点协议使它们可以通信。



图 5-1-5 配置 PPP 协议

实施过程

1. 方法一

➤ RA 上的配置如下。

```
Ruijie#config
Ruijie(config)#hostname RA
RA(config)#int s0/0                                ! 进入 S0/0
RA(config-if-Serial 0/0)#encapsulation ppp          ! 封装 PPP 协议
RA(config-if-Serial 0/0)#ip add 192.168.1.1 255.255.255.252 ! 设置接口 IP 地址
```

➤ RB 上的配置如下。

```
Ruijie#config
Ruijie(config)#hostname RB
RB(config)#int s0/0
RB(config-if-Serial 0/0)#encapsulation ppp          ! 封装 PPP 协议
RB(config-if-Serial 0/0)#ip add 192.168.1.2 255.255.255.252 ! 设置接口 IP 地址
```

2. 方法二

➤ RA 上的配置如下。

```
Ruijie#config
Ruijie(config)#hostname RA
RA(config)#int s0/0
RA(config-if-Serial 0/0)#encapsulation ppp          ! 封装 PPP 协议
RA(config-if-Serial 0/0)#ip add 192.168.1.1 255.255.255.252 ! 设置接口 IP 地址
RA(config-if-Serial 0/0)# peer default ip address 202.202.202.202
! 为对端设备接口分配 IP 地址
```

➤ RB 上的配置如下。

```
Ruijie#config
Ruijie(config)#hostname RB
RB(config)#int s0/0
RB(config-if-Serial 0/0)#encapsulation ppp          ! 封装 PPP 协议
RB(config-if-Serial 0/0)#ip add negotiated          ! 使用对端分配的 IP 地址
```

任务 2 配置路由器广域网链路认证

5.2.1 PPP 协议安全认证

PPP 协议链路协商过程中可以配置认证，客户端会将自己的身份发送给远端的接入服务



器。该阶段使用一种安全验证方式，避免第三方窃取数据，或冒充远程客户接管，与客户端进行连接。在认证完成之前，禁止从认证阶段前进到网络层协议阶段。

如果认证失败，则认证者应该跃迁到链路终止阶段。

在这一阶段里，只有链路控制协议、认证协议和链路质量监视协议的报文是被允许的。在该阶段里接收到的其他的报文被丢弃。PPP 提供了两种可选的身份认证方法：口令验证协议（Password Authentication Protocol, PAP）和挑战握手验证协议（Challenge Handshake Authentication Protocol, CHAP）。

1. PAP

PAP 是一个简单的、实用的身份验证协议，PAP 认证进程只在双方的通信链路建立初期进行。如果认证成功，则在通信过程中不再进行认证。如果认证失败，则直接释放链路。

当双方都封装了 PPP 协议且要求进行 PAP 身份认证，同时它们之间的链路在物理层已激活后，认证客户端（被认证一端）会不停地发送身份认证请求，直到身份认证成功。当认证客户端路由器发送了用户名或口令后，认证服务器会将收到的用户名和口令与本地数据库中的口令信息进行比较，如果正确则身份认证成功，否则认证失败。

PAP 是一种简单的明文验证方式，如图 5-2-1 所示。网络接入服务器（Network Access Server, NAS）要求用户提供用户名和口令，PAP 以明文方式返回用户信息。很明显，这种验证方式的安全性较差，第三方可以很容易地获取被传送的用户名和口令，并利用这些信息与 NAS 建立连接以获取 NAS 提供的所有资源。所以，一旦用户密码被第三方窃取，PAP 无法提供避免受到第三方攻击的保障。措施。

从图 5-2-1 中可以看出，PAP 认证过程经过了两个阶段，通常称为两次握手。

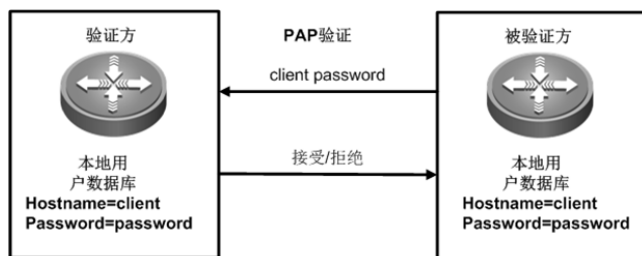


图 5-2-1 PAP 认证

阶段 1：被验证方（远端路由器）发送用户名和口令到验证方。

阶段 2：验证方（中心路由器）对用户名和口令进行认证，根据结果返回接受或拒绝认证请求的信息。

PAP 认证可以在一方进行，即由一方认证另一方的身份，也可以进行双向身份认证。这时，要求被认证的双方都通过对方的认证程序，否则，无法建立二者之间的链路。

PAP 的弱点是用户的用户名和密码是明文发送的，有可能被协议分析软件捕获而导致安全问题。但恰恰是这样，认证只在链路建立初期进行，因此节省了宝贵的链路带宽。

2. CHAP

CHAP 是一种加密的验证方式，能够避免建立连接时传送用户的真实密码，如图 5-2-2 所

示。CHAP 认证比 PAP 认证更安全，因为 CHAP 不在线路上发送明文密码，而是发送经过摘要算法加工过的随机序列，也被称为“挑战字符串”。同时，身份认证可以随时进行，包括在双方正常通信过程中。因此，非法用户就算截获并成功破解了一次密码，此密码也将在一段时间内失效。

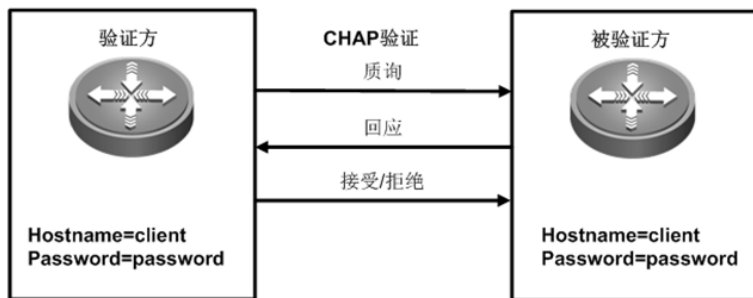


图 5-2-2 CHAP 认证过程

NAS 向远程用户发送一个挑战口令，其中包括会话 ID 和一个任意生成的挑战字串。远程客户必须使用 MD5 单向哈希算法，返回用户名和加密的挑战口令、会话 ID 以及用户口令，其中用户名以非哈希方式发送。

CHAP 对 PAP 进行了改进，不再直接通过链路发送明文口令，而是使用挑战口令以哈希算法对口令进行加密。因为服务器端存有客户的明文口令，所以服务器可以重复客户端进行的操作，并将结果与用户返回的口令进行对照。

CHAP 为每一次验证任意生成一个挑战字符串来防止受到再现攻击。在整个连接过程中，CHAP 将不定时向客户端重复发送挑战口令，从而避免第三方冒充远程客户进行攻击。

CHAP 对系统要求很高，因为需要多次进行身份质询、响应。这需要耗费较多的 CPU 资源，因此只用在安全要求很高的场合。

因为 CHAP 不在线路上发送明文密码，所以 CHAP 认证比 PAP 认证更安全。同 PAP 一样，CHAP 认证可以在一方进行，即由一方认证另一方的身份，也可以进行双向身份认证。这时，要求被认证的双方都通过对方的认证程序，否则，无法建立二者之间的链路。与 PAP 不同的是，这时认证服务器发送的是“挑战”字符串。

5.2.2 配置 PAP 协议安全认证

配置 PAP 认证时，先将接口类型配置为 PPP，再按照以下方法配置。

1. 服务器端

(1) 建立本地口令数据库。

```
ruijie(config)#username name { nopassword | password password }
```

(2) 要求进行 PAP 认证。

```
ruijie(config-if-Serial 0/0)#ppp authentication pap
```

2. 客户端

将用户名和口令发送到对端。

```
ruijie(config-if-Serial 0/0)#ppp pap sent-username username [ password
```



```
password ]
```

5.2.3 配置 CHAP 协议安全认证

配置 CHAP 认证时，先将接口类型配置为 PPP，再按照以下方法配置。

1. 服务器端

(1) 建立本地口令数据库。

```
ruijie(config)#username name {nopassword | password password}
```

(2) 要求进行 CHAP 认证。

```
(config-if-Serial 0/0)#ppp authentication chap
```

2. 客户端

建立本地口令数据库。

```
ruijie(config)#username name {nopassword | password password}
```

[综合实训]：配置 PAP 协议安全认证

网络场景

如图 5-2-3 所示，RA 和 RB 通过 S0/0 相连，通过 PAP 实现双向认证。

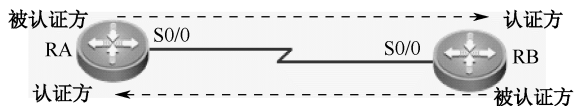


图 5-2-3 配 PAP 双向认证

实施过程

➤ RA 的配置如下。

```
Ruijie#config
Ruijie(config)#hostname RA
RA(config)#username RB password 123
RA(config)#int s0/0
RA(config-if-Serial 0/0)#encapsulation ppp
RA(config-if-Serial 0/0)# ppp authentication pap
RA(config-if-Serial 0/0)# ppp pap sent-username RA password 123
RA(config-if-Serial 0/0)#exit
```

➤ RB 的配置如下。

```
Ruijie#config
Ruijie(config)#hostname RB
RB(config)# username RA password 123
RB(config)#int s0/0
RB(config-if-Serial 0/0)#encapsulation ppp
```

```
RB(config-if-Serial 0/0)# ppp authentication pap
RB(config-if-Serial 0/0)# ppp pap sent-username RB password 123
```

【综合实训】：配置 CHAP 协议安全认证

网络场景

如图 5-2-4 所示，RA 和 RB 通过 S0/0 相连，通过使用 CHAP 配置单向认证。



图 5-2-4 配置 CHAP 认证

实施过程

➤ RA 的配置如下。

```
Ruijie#config
Ruijie(config)#hostname RA
RA(config)#int s0/0
RA(config-if-Serial 0/0)#encapsulation ppp
RA(config-if-Serial 0/0)# ppp chap hostname ruijie
RA(config-if-Serial 0/0)# ppp chap password 123
RA(config-if-Serial 0/0)#exit
```

➤ RB 的配置如下。

```
Ruijie#config
Ruijie(config)#hostname RB
RB(config)# username ruijie password 123
RB(config)#int s0/0
RB(config-if-Serial 0/0)#encapsulation ppp
RB(config-if-Serial 0/0)# ppp authentication chap
RB(config-if-Serial 0/0)#exit
```

任务 3 配置路由器 NAT 技术

5.3.1 路由器 NAT 技术

1. 概述

网络地址转换 (Network Address Translation , NAT) 是将 IP 数据包头中的 IP 地址转换为另一个 IP 地址的过程。

NAT 最初的目的也是通过允许较少的公用 IP 地址代表多数的专有 IP 地址来减缓 IP 地址空间枯竭的速度。在实际应用中，NAT 主要用于实现私有网络访问公共网络的功能。这种通过使用少量的公有 IP 地址代表较多的私有 IP 地址的方式，将有助于减缓可用 IP 地址空间的不足。



图 5-3-1 描述了 NAT 技术在网络中的简单实现。PC1 具有一个私有地址 192.168.1.100，这个地址在互联网上是不被传输的，当 PC1 要访问远程主机 PC2 的时候，数据包要通过一个运行 NAT 技术的路由器。

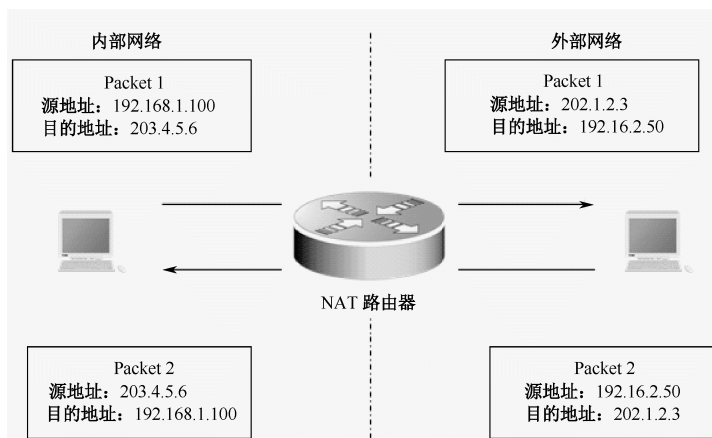


图 5-3-1 NAT 技术对于地址可以进行双向隐藏

路由器把 PC1 的私有地址转换成一个可以在互联网上传输的公有地址 202.1.2.3，然后把数据包转发出去。当 PC2 应答 PC1 的时候，PC2 数据包中的目的地址是 202.1.2.3，当通过路由器接收到 PC2 的目的地址是 202.1.2.3 的数据包时，路由器会把数据包的目的地址转换成 PC1 的私有地址，完成 PC1 和 PC2 的通信。

在上面的例子中，对于 PC1 来讲，本身是不知道 202.1.2.3 这个公有地址的；对于 PC2 来讲，它认为在与 202.1.2.3 这个地址的主机进行通信，并不知道 PC1 的真实地址。所以 NAT 技术对于网络上的终端用户是透明的。

在上面这个例子中，PC1 的地址被转换成 202.1.2.3，PC2 的地址被转换成 203.4.5.6。PC1 认为 PC2 的地址是 203.4.5.6，所以发往 PC2 的数据包的目标的址是 203.4.5.6，PC2 认为 PC1 的地址是 202.1.2.3，所以应答 PC1 的数据包的目的地址是 202.1.2.3。其实 PC1 和 PC2 真实的地址分别是 192.168.1.100 和 192.16.2.50。

2. 工作过程

NAT 技术把地址分成两大部分，即内部地址和外部地址。内部地址分为内部本地（Inside Local，IL）地址和内部全局（Inside Global，IG）地址，外部地址分为外部本地（Outside Local，OL）地址和外部全局（Outside Global，OG）地址。

这四个概念清楚地阐明了代表相同主机的不同地址在 NAT 技术中所处的位置。注意，这里的四个概念是相对于网络中某一台主机来讲的，因为主机处在不同的网络中时 NAT 可以解释为不同的地址。下面来解释这四个基本概念。

- 内部本地地址：在内部网络中分配给主机的私有 IP 地址。
- 内部全局地址：一个合法的 IP 地址，它对外代表一个或多个内部局部 IP 地址。
- 外部本地地址：由其所有者给外部网络上的主机分配的 IP 地址。
- 外部局部地址（Outside Local），外部主机在内部网络中表现出来的 IP 地址。

如图 5-3-2 所示，当内部网络中的一台主机想传输数据到外部网络时，它先将数据包传输到

NAT 路由器上，路由器检查数据包的报头，获取该数据包的源 IP 信息，并从它的 NAT 映射表中找出与该 IP 匹配的转换条目，用所选用的内部全局地址来替换内部本地地址，并转发数据包。

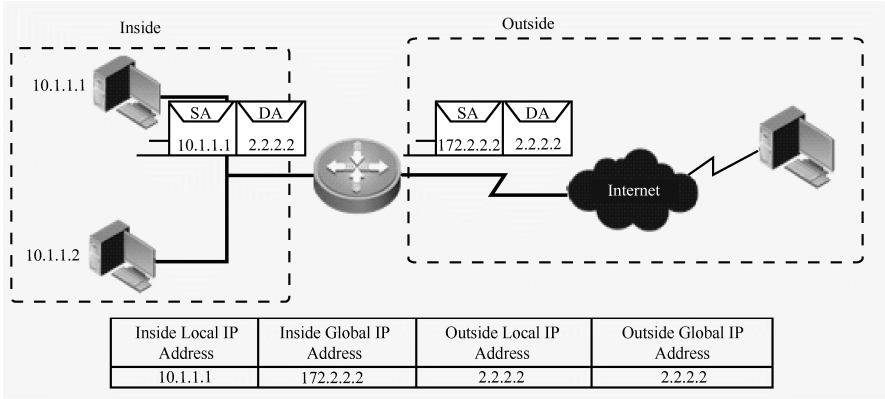


图 5-3-2 NAT 工作原理

当外部网络对内部主机进行应答时，数据包被送到 NAT 路由器上，路由器接收到目的地址为内部全局地址的数据包后，它将用内部全局地址通过 NAT 映射表查找出内部局部地址，然后将数据包的目的地址替换成内部局部地址，并将数据包转发到内部主机。

3. NAT 分类

根据 NAT 的映射方式，NAT 可分为以下几类。

- 静态 NAT，手动建立一个内部 IP 地址到一个外部 IP 地址的映射关系。该方式经常用于企业网的内部设备需要能够被外部网络访问到的场合。
- 动态 NAT，将一个内部 IP 地址转换为一组外部 IP 地址（地址池）中的一个 IP 地址。该方式常用于整个公司共用多个公网 IP 地址访问 Internet 时。

5.3.2 路由器 NAPT 技术

网络地址端口转换（Network Address Port Translation，NAPT）则是把内部地址映射到外部网络的一个 IP 地址的不同端口上。NAPT 是人们比较熟悉的一种转换方式，NAPT 普遍应用于接入设备中，它可以将中小型的网络隐藏在一个合法的 IP 地址后面。

NAPT 与动态地址 NAT 不同，它将内部连接映射到外部网络中的一个单独的 IP 地址上，同时在该地址上加上一个由 NAT 设备选定的 TCP 端口号。

在 Internet 中使用 NAPT 时，所有不同的 TCP 和 UDP 信息流看起来好像来源于同一个 IP 地址。这个优点在小型办公室内非常实用，通过从 ISP 处申请的一个 IP 地址，将多个连接通过 NAPT 接入 Internet。

实际上，许多 SOHO 远程访问设备支持基于 PPP 的动态 IP 地址。这样，ISP 甚至不需要支持 NAPT，就可以做到多个内部 IP 地址共用一个外部 IP 地址接入 Internet，虽然这样会导致信道的一定拥塞，但考虑到节省的 ISP 上网费用和易管理的特点，使用 NAPT 还是很值得的。



5.3.3 配置路由器 NAT 技术

1. 配置静态 NAT

(1) 指定内部接口和外部接口。

```
ruijie(config-if-FastEthernet 0/0)#ip nat { inside | outside}
```

(2) 配置静态转换条目。

```
ruijie(config)#ip nat inside source static local-ip { interface interface |  
global-ip }
```

2. 配置动态 NAT

(1) 指定内部接口和外部接口。

```
ruijie(config-if-FastEthernet 0/0)#ip nat { inside | outside }
```

(2) 定义 IP 访问控制列表。

```
ruijie(config)#access-list access-list-number { permit | deny } address
```

(3) 定义一个地址池。

```
ruijie(config)#ip nat pool pool-name start-ip end-ip { netmask netmask |  
prefix-length prefix-length }
```

(4) 配置动态转换条目。

```
ruijie(config)#ip nat inside source list access-list-number { interface  
interface | pool pool-name}
```

3. 查看操作

```
ruijie#show ip nat translations      ! 显示活动的转换条目  
ruijie# show ip nat statistics      ! 显示转换的统计信息  
ruijie#clear ip nat translation *    ! 清除所有的转换条目
```

5.3.4 配置路由器 NAPT 技术

1. 概述

由于 NAT 实现的是私有 IP 地址和 NAT 的公共 IP 地址之间的转换，那么，私有网中同时与公网进行通信的主机数量就受到 NAT 的公共 IP 地址数量的限制。为了克服这种限制，NAT 被进一步扩展到在进行 IP 地址转换的同时进行 Port 的转换，这就是 NAPT 技术。

NAPT 与 NAT 的区别在于，NAPT 不仅转换 IP 包中的 IP 地址，还对 IP 包中 TCP 和 UDP 的 Port 进行转换。这使得多台私有网主机利用 1 个 NAT 公共 IP 就可以同时和公网进行通信。

2. 配置

(1) 配置动态 NAPT。

指定内部接口和外部接口。

```
ruijie(config-if-FastEthernet 0/0)#ip nat { inside | outside }
```

定义 IP 访问控制列表。

```
ruijie(config)#access-list access-list-number { permit | deny } address
```

定义一个地址池。

```
ruijie(config)#ip nat pool pool-name start-ip end-ip { netmask netmask |
prefix-length prefix-length }
```

配置动态转换条目。

```
ruijie(config)#ip nat inside source list access-list-number { interface
interface | pool pool-name } overload ! 配置“overload”参数则为 NAT，锐捷默认为 NAT
```

(2) 配置静态端口地址转换。

(1) 指定内部接口和外部接口。

```
ruijie(config-if-FastEthernet 0/0)#ip nat { inside | outside }
```

(2) 配置静态端口转换条目。

```
ruijie(config)#ip nat inside source static {tcp | udp} local-ip local-port
{interface interface | global-ip} global-port
```

【综合实训】：配置路由器 NAT 技术

网络场景

如图 5-3-3 所示，校园网中 Router1 为出口路由器，Router1 的 F0/0 口连接核心交换机 G0/24 接口，核心交换机的 G0/1 连接到 PC1 上。Router1 F0/0 的 IP 地址为 192.168.255.254/30，核心交换机的 G0/24 的 IP 为 192.168.255.253/30，核心交换机 VLAN 10 对应的 SVI 口 IP 地址为 192.168.1.254/24，G0/1 口加入 VLAN 10，PC1 的 IP 地址为 192.168.1.1/24，网关为 192.168.1.254，网络使用静态路由。

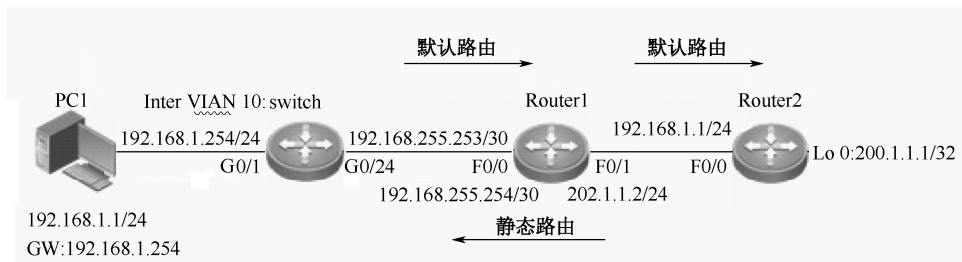


图 5-3-3 NAT 示意图

学校申请一条外网线路，Router1 的 F0/1 口接到外网，公网地址为 202.1.1.0/24 网段，其中 Router1 的 F0/1 口地址为 202.1.1.2/24，网关为 202.1.1.1。在此使用 Router2 充当外网设备，Router2 的 F0/0 地址为 202.1.1.1/24，在 Router2 上配置 interface Lo 0 的地址为 200.1.1.1/32。

具体要求如下。

(1) PC1 能访问外网地址 200.1.1.1。

(2) 校园网中有一台服务器 192.168.1.20/24 需要对外网提供 Web 服务，要将服务器映射到外网。



实施过程

1. 配置 PC 的 IP 地址

配置 PC1 的 IP 地址为 192.168.1.1，网关为 192.168.1.254。

2. 配置交换机和路由器地址

➤ switch 的配置如下。

```
Ruijie>en
Ruijie#config
Ruijie(config)#hostname switch
switch(config)#inter gi 0/24
switch(config-if-GigabitEthernet 0/24)#no switchport
switch(config-if-GigabitEthernet 0/24)#ip address 192.168.255.253
255.255.255.252
switch(config-if-GigabitEthernet 0/24)#exit
switch(config)#vlan 10
switch(config-vlan)#int vlan 10
switch(config-if-VLAN 10)#ip address 192.168.1.254 255.255.255.0
switch(config-if-VLAN 10)#exit
switch(config)#int gi 0/1
switch(config-if-GigabitEthernet 0/1)#switchport access vlan 10
switch(config-if-GigabitEthernet 0/1)#exit
switch(config)#
```

➤ Router1 的配置如下。

```
Ruijie#config
Ruijie(config)#hostname Router1
Router1(config)#inter f 0/0
Router1(config-if-FastEthernet 0/0)# ip address 192.168.255.254
255.255.255.252
Router1(config-if-FastEthernet 0/0)#exit
Router1(config)#int f 0/1
Router1(config-if-FastEthernet 0/1)# ip address 202.1.1.2 255.255.255.0
Router1(config-if-FastEthernet 0/1)#exit
Router1(config)#
```

➤ Router2 的配置如下。

```
Ruijie#config
Ruijie(config)#hostname Router2
Router2(config)#int f 0/0
Router2(config-if-FastEthernet 0/0)#ip address 202.1.1.1 255.255.255.0
Router2(config-if-FastEthernet 0/0)#exit
Router2(config)#int loopback 0
Router2(config-if-Loopback 0)#ip address 200.1.1.1 255.255.255.255
Router2(config-if-Loopback 0)#exit
Router2(config)#
```

3. 配置路由

➤ switch 的配置如下。

```
switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.255.254
```

! 将访问外网数据发给 router1

➤ Router1 的配置如下。

```
Router1(config)#ip route 0.0.0.0 0.0.0.0 202.1.1.1
```

! 将访问外网数据发给 router2

```
Router1(config)#ip route 192.168.0.0 255.255.0.0 192.168.255.253
```

! 将内网数据发给 switch

备注：不需给 Router2 配置静态路由，如果配置可能不做 NAT 也能通信。

4. 配置 NAT

➤ Router1 的配置如下。

```
Router1(config)#int f 0/0
```

```
Router1(config-if-FastEthernet 0/0)#ip nat inside ! 指定内网口
```

```
Router1(config-if-FastEthernet 0/0)#exit
```

```
Router1(config)#int f 0/1
```

```
Router1(config-if-FastEthernet 0/1)#ip nat outside ! 指定外网口
```

```
Router1(config-if-FastEthernet 0/1)#exit
```

```
Router1(config)#access-list 1 permit 192.168.0.0 0.0.255.255
```

! 配置访问控制列表

```
Router1(config)#ip nat pool dingxiligong netmask 255.255.255.0
```

! 配置 NAT 地址池

```
Router1(config-ipnat-pool)#address 202.1.1.3 202.1.1.5
```

```
Router1(config-ipnat-pool)#exit
```

```
Router1(config)#ip nat inside source list 1 pool dingxiligong overload
```

! 配置 NAT 规则

```
Router1(config)#
```

备注：访问控制列表表示数据满足该条件就做 NAT。NAT 地址池表示转换后的地址。

5. 配置端口映射

```
Router1(config)#ip nat inside source static tcp 192.168.1.20 80 202.1.1.6 80
```

备注：使用端口映射将内网相关端口映射到公网的相关端口。一般公网地址要使用未被占用的地址。

6. 验证

(1) PC1 可以访问 200.1.1.1。

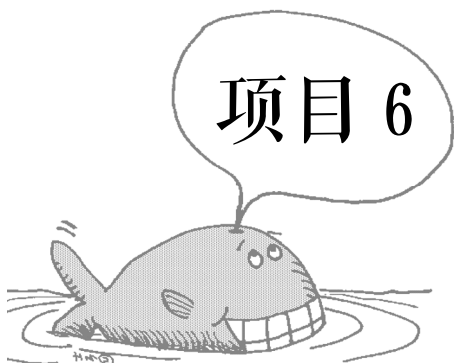
(2) 外网用户可以访问内网服务器。

(3) 查看 NAT 转换表，如图 5-3-4 所示。

```
router1#show ip nat traslation
```

```
router1#show ip nat tr
Pro Inside global      Inside local      Outside local      Outside global
icmp202.1.1.5:655      192.168.1.1:655   200.1.1.1          200.1.1.1
```

图 5-3-4 NAT 信息



配置网络安全技术

任务1 配置交换机登录安全

6.1.1 配置交换机控制台密码

网络安全的隐患是指计算机或其他通信设备，利用网络进行交互时，可能会受到的窃听、攻击或破坏，它是指具有侵犯系统安全或危害系统资源的潜在的环境、条件或事件。计算机网络和分布式系统很容易受到来自非法入侵者和合法用户的威胁。

据国外调查显示，80%的安全破坏事件都是由薄弱的口令引起的，因此为安装在网络中的每台互连设备配置一个恰当的口令，是保护企业内部网络不受侵犯、实施网络安全措施的最基本保护。

1. 概述

基本上网络设备都会有一个控制台接口，通过这个控制台接口，可以对网络设备进行管理。当网络设备第一次使用时，必须通过控制台口对其进行配置。

锐捷交换机和路由器设备默认没有控制台密码，用户可以直接登录，可通过以下方式给交换机设置密码。设置了密码后，用户登录交换机时，需要先输入密码才能进入用户模式。一般还会设置特权密码，这样用户从用户模式到特权模式时还需要输入密码。

2. 配置

```
ruijie(config)#line console 0 ! 进入 Console 接口的配置模式
ruijie(config-line)#password password ! 配置密码
ruijie(config-line)#login ! 加载密码
```

6.1.2 配置路由器控制台密码

1. 设置路由器控制台密码

目前，锐捷路由器及交换机设备使用的操作系统都是 RGOS。因此，路由器设置控制台密码的方法与交换机基本一致，即在控制台模式下配置密码。

2. 设置控制台超时时间

管理员配置设备时，如果已经登录到设备上，若管理员离开计算机后有外人靠近计算机对网络设备进行配置，则可能会出现安全问题。

因此网络中的用户需要给控制台设置超时时间，也就是说，在一段时间没有配置网络设备的会自动退出，如果需要配置，则需再次输入密码。

配置方法如下。

```
ruijie(config)#line console 0
ruijie(config-line)#exec-timeout times ! 设置超时时间（不设置将为系统默认时间）
```

交换机和路由器的配置方法基本相同。

【综合实训】：配置控制台密码

网络场景

如图 6-1-1 所示，正常情况下，PC 接入交换机的 Console 口后就可以登录到交换机的用户模式，通过配置可在管理员从用户模式到特权模式时输入密码，这样无法防止非法用户在用户模式下进行的非法操作。因此，网络中的用户需要配置交换机控制台密码。



图 6-1-1 配置交换机控制台密码

实施过程

1. 配置控制台密码

```
Ruijie> ! 管理员直接进入用户模式
Ruijie>en ! 进入特权模式
Ruijie#config t ! 进入全局配置模式
Ruijie(config)#line console 0 ! 进入控制台模式
Ruijie(config-line)#password dingxiligong ! 配置控制台密码
Ruijie(config-line)#login
Ruijie(config-line)#end
```



```
Ruijie#exit          ! 退出用户模式
Ruijie CON0 is now available
Press RETURN to get started
User Access Verification
Password:            ! 输入控制台密码
Ruijie>              ! 进入用户模式
```

2. 配置控制台的超时时间

```
Ruijie(config)#line console 0          ! 进入控制台
Ruijie(config-line)#exec-timeout 21     ! 设置超时时间
Ruijie(config-line)#exit                ! 退出控制台
```

备注：超时时间默认为 10 分钟，0 代表不退出。

任务 2 配置交换机端口安全

6.2.1 配置交换机端口安全

1. 概述

当网络中的用户组建一个大型的网络时，有时候有很多端口被安放在各个地方，这样网络中的用户就无法保证每个端口都在安全的区域中，或某一个端口比较重要只允许特定的几个网卡接入。这就是基于 MAC 地址的端口安全。

2. 端口安全

网络中的交换机有端口安全功能，利用端口安全这个特性，可以实现网络接入安全，可以通过限制允许访问交换机上某个端口的 MAC 地址以及 IP 地址（可选）来实现严格控制对该端口的输入。当为安全端口打开了端口安全功能并配置了一些安全地址后，除了源地址为这些安全地址的包外，这个端口将不转发其他任何包。此外，还可以限制一个端口上能包含的安全地址的最大个数，如果将最大个数设置为 1，并且为该端口配置一个安全地址，则连接到这个口的工作站（其地址为配置的安全地址）将独享该端口的全部带宽。

3. 端口安全原理

为了增强安全性，可以将 MAC 地址和 IP 地址绑定起来作为安全地址。当然，也可以只指定 MAC 地址而不绑定 IP 地址。

如果一个端口被配置为安全端口，当其安全地址的数目已经达到允许的最大个数后，当该端口收到一个源地址不属于端口上的安全地址的包时，一个安全违例将产生。当安全违例产生时，可以选择多种方式来处理违例，如丢弃接收到的数据包、发送违例通知或关闭相应端口等。

当设置了安全端口上安全地址的最大个数后，可以使用下面几种方式加满端口上的安全地址。

可以使用接口配置模式下的命令 “switchport port-security mac-address mac-address [ip-

address ip-address] ”来手工配置端口的所有安全地址。

也可以让该端口自动学习地址，这些自动学习到的地址将变成该端口上的安全地址，直到达到 IP 最大个数。需要注意的是，自动学习的安全地址均不会绑定地址，如果在一个端口上已经配置了绑定 IP 地址的安全地址，则将不能再通过自动学习来增加安全地址。

网络中的用户都知道每个网络设备的端口或每块网卡都有全球唯一的 MAC 地址，交换机允许网络中的用户在某个端口上指定只允许某个或某几个 MAC 地址接入来保护这个端口，也可以通过一台安全服务器来允许或拒绝一组 MAC 地址的接入。

端口安全主要有以下两种作用。

- 限制交换机端口能接入的最大主机数。
- 根据需要针对端口绑定用户地址。

当用户发出不符合交换机端口安全的数据时，交换机会进行违例处理，方法如下。

- Protect: 当安全地址个数满后，安全端口将丢弃所有新接入的用户数据流。该处理模式为默认的对违例的处理模式。
- Restrict: 当违例产生时，将发送一个 Trap 通知。
- Shutdown: 当违例产生时，将关闭端口并发送一个 Trap 通知。

3. 配置端口安全

(1) 开启端口安全。

```
Switch(config-if-FastEthernet 0/1)#switchport port-security
```

(2) 配置安全策略。其中一个方式是配置最大安全地址数。

```
Switch(config-if-FastEthernet 0/1)#switchport port-security maximum number
```

一个千兆接口上最多支持 120 个同时申明 IP 地址和 MAC 地址的安全地址。

(3) 绑定用户信息。

- 针对端口进行 MAC 地址绑定（只绑定并检查二层源 MAC）：

```
Switch(config-if-FastEthernet 0/1)#switchport port-security mac-address  
mac-address vlan vlan-id
```

建议一个安全端口上的安全地址的格式保持一致，即一个端口上的安全地址或者全是绑定了 IP 地址的安全地址，或者都是不绑定 IP 地址的安全地址。如果一个安全端口同时包含这两种格式的安全地址，则不绑定 IP 地址的安全地址将失效（绑定 IP 地址的安全地址优先级更高），这时如果想使端口上不绑定 IP 地址的安全地址生效，则必须删除端口上所有绑定了 IP 地址的安全地址。

- 针对端口绑定 IP（只绑定并检查源 IP）：

```
Switch(config-if-FastEthernet 0/1)#switchport port-security binding ip-  
address
```

- 针对端口绑定 IP+MAC（绑定并检查源 MAC 和源 IP）：

```
Switch(config-if-FastEthernet 0/1)#switchport port-security binding mac-  
address vlan vlan-id ip-address
```

(4) 设置违例方式。

```
Switch(config-if-FastEthernet 0/1)#switchport port-security violation { protect  
| restrict | shutdown }
```

如果上述违例方式设为 shutdown 且出现违例后，要恢复端口的操作，即：



```
Switch(config)#errdisable recovery
```

6.2.2 配置交换机保护端口安全

1. 概述

有些应用环境下，要求一台交换机上的有些端口之间不能互相通信。在这种环境下，这些端口之间的通信，不管是单址帧，还是广播帧，或者是多播帧，都只能通过三层设备进行通信。此时可以使用保护端口。

在将某些端口设为保护口之后，保护口之间无法互相通信，保护口与非保护口之间已经可以正常通信。

2. 配置

在接口下将其配置为保护口：

```
switch(config-if-FastEthernet 0/1)#switchport protected
```

查看信息的命令如下：

```
switch#show interfaces switchport
```

6.2.3 配置交换机镜像端口安全

1. 概述

在网络中监视进出网络的所有数据包，供安装了监控软件的管理服务器抓取数据，了解网络安全状况，如网吧需提供此功能把数据发往公安部门审查；而企业出于信息安全、保护公司机密的需要，也迫切需要端口镜像技术。在企业中用端口镜像功能，可以很好地对企业内部的网络数据进行监控管理，在网络出现故障时，可以做到很好地故障定位。

2. 端口镜像

端口镜像主要用于监控，主要是把交换机一个或多个端口的数据镜像到另一个端口的方法。也就是说，交换机把某一个端口接收或发送的数据帧完全相同地复制给另一个端口。其中被复制的端口称为镜像源端口，复制的端口称为镜像目的端口。

镜像是将交换机某个端口的流量复制到另一个端口（镜像端口），并进行监测。

交换机的镜像技术是将交换机某个端口的数据流量，复制到另一个端口（镜像端口）进行监测的安全防范技术。大多数交换机支持镜像技术，称为 Mirroring 或 Spanning，默认情况下交换机上的这种功能是被屏蔽的。

通过配置交换机端口镜像，允许管理人员设置监视管理端口，监视被监视的端口的数据流量，将复制到镜像端口的数据通过 PC 上安装的网络分析软件进行查看。通过对捕获到的数据进行分析，可以实时查看被监视端口的情况。场景如图 6-2-1 所示。

2. 配置

大多数交换机支持镜像技术，这可以方便地对交换机进行故障诊断。通过分析故障交换机的数据包信息，了解故障的原因。这种通过一台交换机监控同网络中另一台的过程，称之为“Mirroring”或“Spanning”。

(1) 配置源端口。

```
switch(config)#monitor session session source interface xx
```

(2) 配置镜像目的端口。

```
switch(config)#monitor session session destination interface xx switch
```

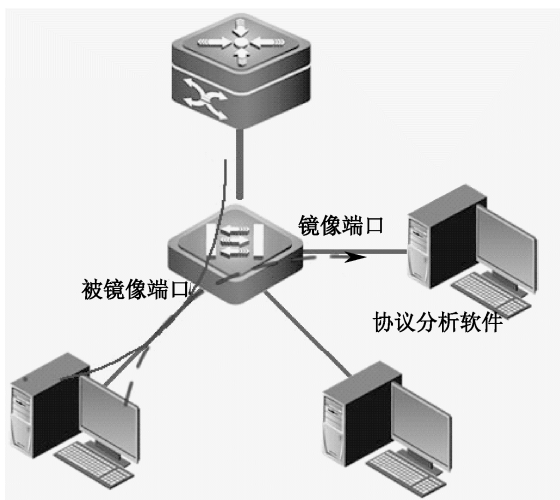


图 6-2-1 端口镜像拓扑

需要注意的是，源端口与目的端口的 session 数量要一致。

如果把某个接口配置为镜像目的的口，则该接口无法通信。

如果要想让这个接口在接收其他口数据的同时能处理自身的数据，则需要在后面添加“switch”参数。

【综合实训】：配置交换机端口安全

网络场景

如图 6-2-2 所示，两个房间的用户接到 Switch 的 F0/1 和 F0/2 口，其中一个房间由于用户过多，所以使用 Hub 进行连接。正常情况下，PC1 和 PC2 可以通信。

为保证网络安全，要求 F0/1 下不能超过 10 个用户，特别要求在 F0/2 下必须使用 PC2 连接且 PC2 的 IP 地址为 192.168.10.2，MAC 地址为 00-1b-b3-02-12-18。如果出现问题，则将接口直接关闭。

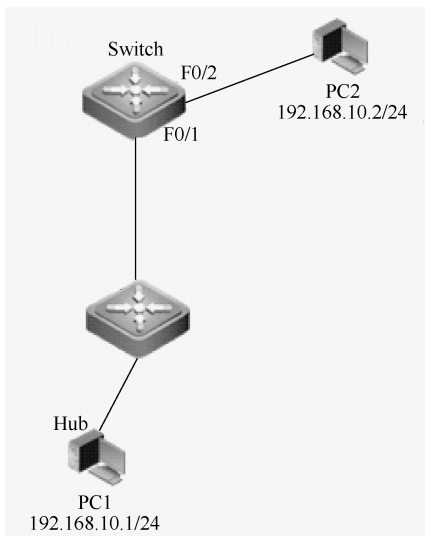


图 6-2-2 交换机端口安全示例

实施过程

1. 配置

```
Ruijie#config
Ruijie(config)#hostname switch
switch(config)#int f 0/1
switch(config-if-FastEthernet 0/1)#switchport port-security
! 开启端口安全功能
switch(config-if-FastEthernet 0/1)#switchport port-security maximum 10
! 端口下最多学习 10 个 MAC 地址
switch(config-if-FastEthernet 0/1)#switchport port-security violation
shutdown
! 出现问题时，将接口关闭

switch(config-if-FastEthernet 0/1)#exit
switch(config)#int f 0/2
switch(config-if-FastEthernet 0/2)#switchport port-security
! 开启端口安全
switch(config-if-FastEthernet 0/2)#switchport port-security binding 001b.
b302.1218 vlan 1 192.168.10.2 ! 端口绑定上网用户的 MAC 地址、IP 地址、VLAN 等
switch(config-if-FastEthernet 0/2)#switchport port-security violation
shutdown
! 出现问题时，将接口关闭

switch(config-if-FastEthernet 0/2)#exit
switch(config)#
```

2. 验证

- (1) 在交换机 F0/1 口下连接超过 10 台 PC，则超出限制的 PC 无法连接到网络。
- (2) 将 F0/2 口下的 PC 换成其他 PC 或修改该 PC 的 IP 地址，则该 PC 无法连接到网络。
- (3) 如果出现 PC 数量超过限制数量或修改地址的情况，则该接口被关闭。

【综合实训】：配置交换机保护端口

网络场景

如图 6-2-3 所示，PC1 和 PC2 连接在交换机的 F0/1 和 F0/2 口，Server 连接在 G0/25 口。要求两台 PC 都能访问服务器但两台 PC 不能互访。

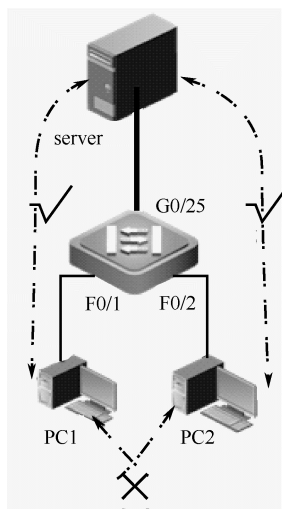


图 6-2-3 交换机保护端口配置

实施过程

1. 配置交换机

```
Ruijie#config
Ruijie(config)#hostname switch
switch(config)#int range f 0/1-2
switch(config-if-range)#switchport protected    ! F0/1 和 F0/2 口配置为保护端口
switch(config-if-range)#exit
```

2. 验证

- (1) PC1 和 PC2 不能通信，但 PC 可以和服务器通信。
- (2) 查看信息，如图 6-2-4 所示。



```
switch#show interfaces switchport
```

Interface	Switchport	Mode	Access	Native	Protected	VLAN lists
FastEthernet 0/1	enabled	ACCESS	1	1	Enabled	ALL
FastEthernet 0/2	enabled	ACCESS	1	1	Enabled	ALL
FastEthernet 0/3	enabled	ACCESS	1	1	Disabled	ALL
FastEthernet 0/4	enabled	ACCESS	1	1	Disabled	ALL
FastEthernet 0/5	enabled	ACCESS	1	1	Disabled	ALL

图 6-2-4 保护端口信息

【综合实训】：配置交换机端口镜像

网络场景

如图 6-2-5 所示，PC1 和 PC2 连接在交换机的 F0/1 和 F0/2 口，Server 连接在 G0/25 口。其中 PC2 为管理员，目前要求管理员可以看到 PC1 的所有上网信息。

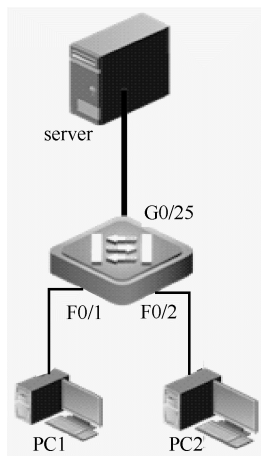


图 6-2-5 端口镜像示意图

实施过程

1. 配置端口镜像

```
Ruijie#config
Ruijie(config)#hostname switch
switch(config)#monitor sess 1 source inter f 0/1      ! 设置镜像源端口
switch(config)#monitor sess 1 dest int f 0/2 switch  ! 设置镜像目的端口
```

备注：若镜像目的端口加“switch”参数，则在查看其他端口数据的过程中其也可以上网。

2. 验证

在 PC2 上开启抓包软件，在 PC1 上访问服务器，则 PC1 的数据 PC2 也能收到。

任务 3 配置编号访问控制列表安全

6.3.1 配置标准访问控制列表

1. 概述

对于许多网管员来说，配置访问控制列表（Access Control Lists，ACL）。是一件经常性的工作，可以说，以太网设备的访问控制列表是网络安全保障的第一道关卡。访问控制列表提供了一种机制，它可以控制和过滤通过路由器或交换机的不同接口，去往不同方向的信息流。

这种机制允许用户使用访问控制列表来管理信息流，以制定内部网络的相关策略。通过 ACL 可以限制网络中的通信数据类型及网络的使用者。ACL 在数据流通过路由器或交换机时对其进行分类过滤，并对从指定接口输入的数据流进行检查，根据匹配条件决定是允许（Permit）其通过还是丢弃（Deny）。

2. 访问控制列表

ACL 最直接的功能便是包过滤。通过访问控制列表可以在路由器、三层交换机上进行网络安全属性配置，可以实现对进入到路由器、三层交换机的输入数据流的过滤。过滤输入数据流的定义可以基于网络地址、TCP/UDP 的应用等。

IP ACL 安全技术简单地说就是数据包过滤技术。网络管理人员通过配置网络设备，来实施对网络中通过的数据包的过滤，从而实现对网络资源的安全访问控制。IP ACL 安全实施的内容是编制一张规则检查表，这张表中包含了很多简单指令规则，告诉设备哪些数据包可以接收，哪些数据包需要被拒绝。

3. ACL 的类型

安装在网络中的三层设备，按照编制完成的 IP ACL 中的指令顺序，依次检查、执行这些规则，处理每一个进入或输出端口的数据包，实现对网络中的数据包的过滤。通过在网络设备上灵活配置 IP ACL，以作为一种网络控制工具，过滤流入和流出数据包可以确保网络的安全，因此有时也把 IP ACL 称为软件防火墙，它具有和防火墙一样的保护功能。

最为常见的 IP ACL 使用编号来进行区分，一般可以分为两类：标准访问控制列表（Standard ACL）和扩展访问控制列表（Extended ACL）。在规则中使用不同的编号区别它们，其中标准访问控制列表的编号取值范围为 1 ~ 99；扩展访问控制列表的编号取值范围为 100 ~ 199。

两种编号的 IP ACL 的区别如下：标准的编号 IP ACL 只匹配、检查数据包中携带的源地址信息；扩展编号 IP ACL 不仅仅匹配数据包中的源地址信息，还检查数据包的目的地址，以及数据包的特定协议类型、端口号等。扩展访问控制列表规则大大扩展了网络设备对三层数据流的检查细节，为网络的安全访问提供了更多的访问控制功能。



4. ACL 组成

一个 ACL 由一系列的表项组成，ACL 中的每个表项称之为存取控制项（Access Control Entry，ACE），主要的动作为允许和拒绝；主要的应用方法是入栈（In）应用和出栈（Out）应用，如图 6-3-1 所示。

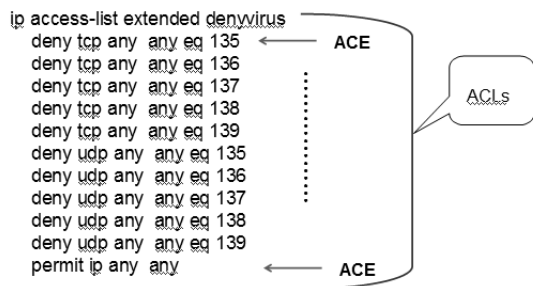


图 6-3-1 ACL 实例

ACE 主要包含识别字段和动作两部分。

- 识别字段：数据的特征如果和该字段完全匹配，则说明匹配了 ACE 条目。
- 动作：常见动作有 Permit 和 Deny 两个。当数据匹配后执行相关操作。

按 ACE 的编号依次匹配，当数据匹配了某个 ACE 时，执行相关动作并退出 ACL。如果不匹配 ACE，则不执行相关动作并继续向下匹配。如果所有 ACE 都不匹配，则默认执行 Deny 动作。

5. 部署标准 ACL

标准 ACL，只检查收到的 IP 数据包中的源 IP 地址信息，以控制网络中数据包的流向。在安全设施的过程中，如果要阻止来自某一特定网络中的所有通信流，或者允许来自某一特定网络的所有通信流，可以使用标准访问控制列表来实现。

基于编号的标准访问控制列表的重要特征如下：通过编号 1~99 来区别不同的 ACL；通过检查 IP 数据包中的源地址信息来区别不同的 ACL。数据包在通过网络设备时，设备解析 IP 数据包中的源地址信息，对匹配成功的数据包采取拒绝或允许操作。

在编制标准 IP ACL 规则时，使用编号 1~99，区别同一设备不同的 IP ACL 列表条数。

(1) 配置标准 ACL。

```
ruijie(config)#access-list number {deny | permit} 源地址
```

(2) 将 ACL 应用到接口。

```

ruijie(config)#interface interface-id
ruijie(config-if-FastEthernet 0/1)#ip access-group number {int | out}
    
```

在此过程中有以下要点。

- 同一个 ACL 可写多条 ACE，可以重复上述写法，但 ACL 的编号要相同。
- 标准访问控制列表的编号是 1~99，1300~1999。
- 配置识别字段时如果匹配所有，则可以写“any”；匹配一个 IP 地址，则可写“host IP 地址”；如果匹配一个网段，则可以使用“网络号加反掩码”的方式。
- 在调用时需写明数据的方向。

6.3.2 配置扩展访问控制列表

1. 概述

扩展访问控制列表相对标准访问控制列表来说更加灵活。使用标准访问控制列表只能通过源 IP 地址控制，如果源地址满足条件，则无论其他字段如何配置数据都满足条件。而使用扩展访问控制列表只有当源 IP、目的 IP、协议等都满足条件数据时才进行匹配。

2. 扩展访问控制列表

基于编号的扩展访问控制列表的重要特征如下：通过编号 100 ~ 199 来区别不同的 IP ACL；不仅检查数据包源 IP 地址，还检查数据包中目的 IP 地址、源端口、目的端口、建立连接和 IP 优先级等特征信息。

数据包在通过网络设备时，设备解析 IP 数据包中的多种类型信息特征，对匹配成功的数据包采取拒绝或允许操作。

扩展访问控制列表在 IP 数据包的过滤方面增加了更多的精细度控制，具有比标准 IP ACL 更强大的数据包检查功能。扩展 ACL 不仅检查数据包源 IP 地址，还检查数据包中目的 IP 地址、源端口、目的端口、建立连接和 IP 优先级等特征信息。

和标准 ACL 相比，扩展 ACL 也存在一些缺点：配置管理难度加大，考虑不周容易限制正常访问；扩展 ACL 会消耗路由器更多的 CPU 资源。所以，中低档路由器进行网络连接时，应尽量减少扩展 ACL 条数，以提高工作效率。

3. 部署扩展 ACL

(1) 配置 ACL。

```
ruijie(config)#access-list number {deny | permit} 协议 源地址 [eq 源端口] 目的地址[eq 目的端口]
```

(2) 调用。

```
ruijie(config)#interface interface-id
ruijie(config-if-FastEthernet 0/1)#ip access-group number {int | out}
```

在此过程中有以下要点。

- 同一个 ACL 可写多条 ACE，可以重复上述写法，但 ACL 的编号要相同。
- 扩展访问控制列表的编号是 100 ~ 199，2000 ~ 2699。
- 配置识别字段时如果匹配所有，则可以写“any”；匹配一个 IP 地址，则可写“host IP 地址”；如果匹配一个网段，则可以使用“网络号加反掩码”的方式。
- 协议可为 IP、TCP、UDP 等，如果是 TCP 或 UDP 还可以加端口。
- 在调用时需写明数据的方向。

6.3.3 配置时间访问控制列表

1. 概述

基于时间的访问控制列表技术，是标准访问控制列表和扩展访问控制列表基础上的扩展，通过在规则配置中加入有效的时间范围，来更有效地控制网络在时间上的限制范围。



通过时间的 ACL 需要先定义一个时间范围，然后在原来各种访问控制列表的基础上应用它；通过它可以根据一天中不同时间，或者根据一周中的不同日期控制网络范围。例如，在学校网络中，希望上课时禁止学生访问学校服务器，而下课时允许学生访问。

基于时间的 IP ACL，对于编号 IP ACL 和名称 IP ACL 均适用。

实现所配置的 ACL 只在一个特定的时间段内生效，如在办公时间（9:00 ~ 18:00）只允许访问 Web 网页，其他应用则被禁止。

除了办公时间外，任何网络应用都可以使用。这时需要配置基于时间的 ACL，再将时间信息调用到相关 ACE 条目上。

2. 定义时间 IP ACL 规则

创建基于时间的 IP ACL，需要依据两个要点：使用参数 time-range 定义一个时间段；编制编号 IP ACL 或者名称 IP ACL，再将 IP ACL 规则和时间段结合起来应用。

ACL 需要和时间段结合起来应用，即基于时间的 ACL。事实上，基于时间的 ACL 只是在 ACL 规则后，使用 time-range 选项为此规则指定一个时间段，只有在此时间范围内此规则才会生效，各类 ACL 规则均可以使用时间段。

时间段可分为三种类型：绝对（Absolute）时间段、周期（Periodic）时间段和混合时间段。

- 绝对时间段：表示一个时间范围，即从某时刻开始到某时刻结束，如 1 月 5 日早晨 8 点到 3 月 6 日早晨 8 点。
- 周期时间段：表示一个时间周期，如每天早晨 8 点到晚上 6 点，或每周一到每周五的早晨 8 点到晚上 6 点。
- 混合时间段：可以将绝对时间段与周期时间段结合起来，称为混合时间段，如 1 月 5 日到 3 月 6 日每周一至周五早晨 8 点到晚上 6 点。

在全局模式下，使用如下命令创建并配置时间段，当执行此命令后，系统将进入到时间段配置模式。

3. 配置方法

（1）正确配置设备时间。

```
ruijie#clock set XX:XX:XX month day year
```

（2）定义时间段。

```
ruijie(config)#time-range name  
ruijie(config-time-range)#periodic 时间段
```

（3）为 ACL 中特定 ACE 关联定义好的时间段。

```
ruijie(config)#access-list number {deny | permit} 条件 time-range name
```

需要注意以下几点。

- 设置时间段时，常见的参数有：Daily，每天；Friday，星期五；Monday，星期一；Saturday，星期六；Sunday，星期日；Thursday，星期四；Tuesday，星期二；Wednesday，星期三；Weekdays，周一到周五；Weekend，周六和周日。还可添加时间。
- 时间 ACL 可配置在扩展访问控制列表和标准访问列表的 ACE 中。
- 当时间在其范围内，对应的 ACE 生效。

类似这种基于时间的应用控制，由于实际中涉及的应用类型比较复杂，因此多在出口位

置采用专用的设备进行控制。

【综合实训】：配置编号标准访问控制列表

网络场景

如图 6-3-2 所示，PCA 连接在路由器的 F0/1 口，PCB 连接在路由器的 F0/2 口。PCA 的 IP 地址为 192.168.10.1/24，PCB 的 IP 地址是 192.168.20.1/24。

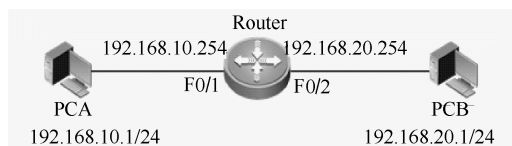


图 6-3-2 配置编号标准访问控制列表

路由器 F0/1 口 IP 地址为 192.168.10.254/24，充当 PCA 的网关；路由器 F0/2 口 IP 地址为 192.168.20.254/24，充当 PCB 的网关。正常情况下，两台 PC 可以通信，要求 PCA 和 PCB 不能通信但 PCA 换成同网段其他设备时可以和 PCB 通信。

实施过程

1. 配置计算机的 IP 及网关

按图 6-3-2 配置计算的 IP 地址及网关。

2. 配置交换机的 IP 地址

```

Ruijie#config
Ruijie(config)#hostname router
router(config)#int f0/1
router(config-if-FastEthernet 0/1)#ip address 192.168.10.254 255.255.255.0
router(config-if-FastEthernet 0/1)#exit
router(config)#int f0/2
router(config-if-FastEthernet 0/2)#ip address 192.168.20.254 255.255.255.0
router(config-if-FastEthernet 0/2)#exit
router(config)#
  
```

3. 配置编号标准访问控制列表

```

router(config)#access-list 1 deny host 192.168.10.1
! 该表不允许源地址为 192.168.10.1 的数据通过
router(config)#access-list 1 permit 192.168.10.0 0.0.0.255
! 但允许 192.168.10.0/24 其他地址数据通过
  
```

备注：该 ACL 可以配置多条规则，但标号要相同。



4. 部署 ACL

```
router(config)#int f 0/1
router(config-if-FastEthernet 0/1)#ip access-group 1 in
! 将访问控制列表用到 F0/1 口的入方向
router(config-if-FastEthernet 0/1)#exit
router(config)#
```

备注：可调用到 F0/2 的 out 方向。

5. 验证

PC1 不能 Ping 通 PC2，但将 PC1 的 IP 地址变为 192.168.10.5 后可以和 PC2 通信。

【综合实训】：配置标准访问控制列表

网络场景

如图 6-3-3 所示，PC1、PC2 和 PC3 连接在交换机 F0/1、F0/2 和 F0/3 口上。PC1 的 IP 地址为 192.168.1.1/24、PC2 的 IP 地址为 192.168.1.2/24、PC3 的 IP 地址为 192.168.1.3/24。

需要保证 PC1 和 PC3 不能通信，PC2 和 PC3 可以通信，PC1 和 PC2 也可以通信。

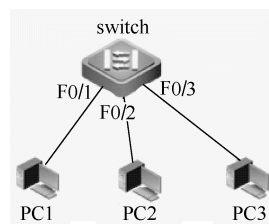


图 6-3-3 配置标准访问控制列表

实施过程

1. 配置计算机的 IP 地址

按上方配置 PC 的 IP 地址。

2. 配置访问控制列表

```
Ruijie#config
Ruijie(config)#hostname switch
switch(config)#access-list 101 deny ip host 192.168.1.1 host 192.168.1.3
switch(config)#access-list 101 permit ip host 192.168.1.1 host 192.168.1.2
switch(config)#
```

备注：可简化配置，即配置 “permit ip host 192.168.1.1 host 192.168.1.2” 实现该功能。

3. 应用到 F0/1 的 in 方向

```
switch(config)#int f 0/1
switch(config-if-FastEthernet 0/1)#ip access-group 101 in
```

4. 验证

PC1 不能和 PC3 通信、PC1 可以和 PC2 通信、PC2 可以和 PC3 通信。

【综合实训】：配置时间访问控制列表

网络场景

如图 6-3-4 所示，PC1、PC2 连接在交换机 F0/1、F0/2 口上。PC1 的 IP 地址为 192.168.1.1/24、PC2 的 IP 地址为 192.168.1.2/24。

每天上午 9:00 ~ 12:00 两个用户可以通信，其他时间不能通信。

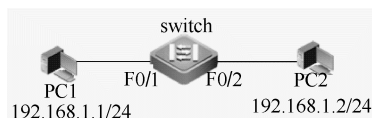


图 6-3-4 配置时间访问控制列表

实施过程

1. 配置计算机的 IP 地址

按上文配置 PC 的 IP 地址。

2. 配置时间段

```
Ruijie#config
Ruijie(config)#hostname switch
switch(config)#time-range dingxiligongxuexiao
switch(config-time-range)#periodic weekdays 9:00 to 12:00
switch(config-time-range)#exit
```

3. 配置访问控制列表

```
switch(config)#access-list 1 permit host 192.168.1.1 time-range dingxiligongxuexiao
```

4. 应用到 F0/1 的 in 方向

```
switch(config)#int f 0/1
switch(config-if-FastEthernet 0/1)#ip access-group 1 in
```

备注：需要先保证时间正确。

4. 验证

在规定时间内 PC1 可以 Ping 通 PC2。



任务4 配置名称访问控制列表

6.4.1 配置标准名称访问控制列表安全

1. 概述

基于编号的 ACL 是访问控制列表发展早期应用最为广泛的技术之一。其中，标准的 IP ACL 使用数字编号 1~99 和 1300~1999；扩展 IP ACL 使用数字编号 100~199 和 2000~2699。

但使用编号 IP ACL 不容易识别，数字编号不容易区分，有耗尽的可能，特别是基于编号的 IP ACL 在修改上非常不方便。因此，近些年来，随着设备的性能改善以及技术的进步，基于名称的 IP ACL 应运而生，基于名称的 IP ACL 在技术开发上避免了以上基于编号的 IP ACL 在应用上的不足。

2. 基于名称的访问控制列表规则

基于名称的 IP ACL 在规则编辑上使用了一组字符串，来标识编制完成的安全规则，具有“见名识意”的效果，方便了网络管理人员管理。除了命名，以及在编写规则的语法上稍有不同外，其他诸如检查的元素、默认的规则等都与编号的访问控制列表相同。

此外，基于名称的 IP ACL 同样分为标准 IP ACL 和扩展 IP ACL。与编号 IP ACL 相比，名称 IP ACL 的主要优点如下。

- 允许管理员给 ACL 指定一个描述性的名称，能“见名识意”。
- 允许管理生成超过 99 个的标准 ACL 或超过 100 个的扩展 ACL，这是可以建立的 ACL 数的初始限制。
- 引入有序的 ACL，允许插入和删除特定的 ACL 条目。

基于编号的 IP ACL 有一个弊端，设置完成 IP ACL 的规则后，发现其中某条有问题，希望修改或删除的话，只能将全部 IP ACL 信息都删除，也就是说，修改一条或删除一条，都会影响到整个 IP ACL 列表，给其带来了繁重的负担。

基于名称的 IP ACL 在编制完成后，可以方便地修改。应该使用基于名称的 IP ACL 进行管理，这样可以减轻很多后期维护的工作，方便随时调整 IP ACL 规则。

3. 配置方案

创建名称 IP ACL 与编号 IP ACL 的语法命令不同，名称 IP ACL 使用 `ip access-list` 命令开头。在配置标准 ACL 时，可使用编号来命名 ACL。为了表明 ACL 的作用，也可以用字母表示 ACL。

当使用字母表示 ACL 时写法如下。

```
ruijie(config)#ip access-list standerd name      ! 创建 IP 的标准访问控制列表
ruijie(config-acl)# {deny | permit} 源地址      ! 在列表中配置 ACE
```

- 使用这种写法时，名称可以使用数字或字母。
- 可在列表内加多条 ACE。

- ACE 中的内容和使用编号一致。
- 调用时使用的名称和其使用的名称一致。

在接口模式中，应用名称 IP ACL 与应用编号 IP ACL 的方法和命令一样，只是此处将编号替换为名称“name”了。

```
Router(config)#ip access-group name { in | out }
! name 表示 ACL 名称，与之前创建的 ACL 名称要保持一致
```

6.4.2 配置扩展名称访问控制列表安全

创建扩展的名称 IP ACL 与标准 IP ACL 的语法命令相同，也使用 ip access-list 命令开头。在配置扩展 ACL 时，也可以用字母表示 ACL。

使用“ip access-list extended”命令建立命名的扩展 ACL，后面跟 ACL 名称，执行该命令时，进入子配置模式，输入 permit 或 deny 语句，其语法和编号的 ACL 相同，并且支持相同的选项。

如果使用字母表示 ACL，其写法如下。

```
ruijie(config)#ip access-list extended name      ! 创建 IP 扩展访问控制列表
ruijie(config-acl)# {deny | permit} 协议 源地址 [eq 源端口] 目的地址 [eq 目的端口]
! 在列表中配置 ACE
```

备注：使用这种写法时，名称可以使用数字或字母；可在列表内加多条 ACE；ACE 中的内容和使用编号一致。

在接口应用名称 ACL 与应用编号 ACL 的方法和命令一样，只要将编号替换为名称“name”即可。

```
ip access-group name { in | out }
```

这里的“name”表示名称 IP ACL 的名称，要与之前创建的名称 IP ACL 的名称保持一致。

【综合实训】：配置名称访问控制列表

网络场景

如图 6-4-1 所示，网段 172.16.1.0 中的主机能够访问 172.17.1.1 中的 FTP 服务和 Web 服务，而对该服务器的其他服务禁止访问，但可以访问 172.17.1.2 的任何服务。

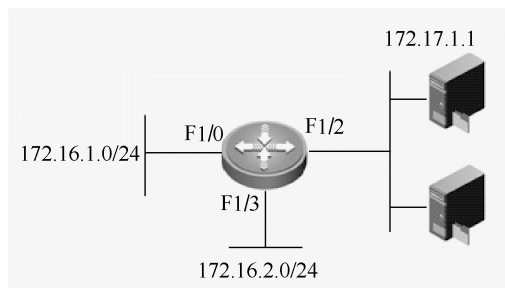


图 6-4-1 配置名称访问控制列表



实施过程

1. 配置计算机 IP 和网关

按图 6-4-1 配置计算机的 IP 地址和网关。

2. 地址配置

```
Ruijie#config
Ruijie(config)#hostname router
router(config)#int fal/0
router(config-if-FastEthernet 1/0)#ip address 172.16.1.254 255.255.255.0
router(config-if-FastEthernet 1/0)#exit
router(config)#int fal/1
router(config-if-FastEthernet 1/1)#ip address 172.16.2.254 255.255.255.0
router(config-if-FastEthernet 1/0)#exit
router(config)#int fal/2
router(config-if-FastEthernet 1/0)#ip address 172.17.1.254 255.255.255.0
router(config-if-FastEthernet 1/0)#exit
router(config)#
```

3. 配置访问控制列表

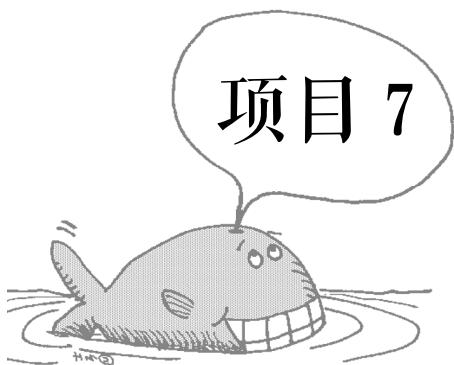
```
router(config)#ip access-list extended dingxi
router(config-ext-nacl)#permit tcp 172.16.1.0 0.0.0.255 host 172.17.1.1 eq www
router(config-ext-nacl)#permit tcp 172.16.1.0 0.0.0.255 host 172.16.1.1 eq ftp
router(config-ext-nacl)#permit tcp 172.16.1.0 0.0.0.255 host 172.16.1.1 eq
ftp-data
router(config-ext-nacl)#permit ip 172.16.1.0 0.0.0.255 host 172.16.1.2
router(config-ext-nacl)#exit
```

4. 调用接口

```
router(config)#int fal/0
router(config-if-FastEthernet 1/0)#ip access-group dingxi in
router(config-if-FastEthernet 1/0)#exit
```

5. 验证

网段 172.16.1.0 中的主机能够访问 172.17.1.1 中的 FTP 服务和 Web 服务，而对该服务器的其他服务禁止访问，但可以访问 172.17.1.2 的任何服务。



配置防火墙设备

任务 1 配置防火墙基础技术

7.1.1 防火墙登录配置

1. 概述

RG-WALL1600 下一代防火墙系列（NGFW）是面向云计算、数据中心和园区及企业网出口用户开发的新一代高性能防火墙设备。它的功能特性如下。

- 采用 RG-Slab 锐捷网络安全研究组最新发表的 HiSpeed 安全处理算法，突破硬件处理器对应用层安全检测的性能瓶颈，能以高性能提供深度状态检测、外部攻击防范、内网安全、流量监控、邮件过滤、网页过滤、应用层过滤等功能，有效保障了网络的安全。
- 提供多种智能分析和手段，支持邮件告警和日志告警，提供网络管理监控，协助网络管理员完成网络的安全管理。
- 支持基于用户、资源、应用的访问控制。
- 支持 GRE、L2TP、IPSec 和 SSL 等多种 VPN 业务，可以构建多种形式的 VPN。
- 提供强大的路由能力，支持 NAT、静态/RIP/OSPF/路由策略及策略路由。
- 支持双机热备（两台 NGFW 互相冗余备份），支持 Active/Active（主-主模式）和 Active/Standby（主-备模式）两种工作模式以及丰富的 QoS 特性，充分满足客户对网络高可靠性的要求。

NGFW 系列目前共有如下型号：RG-WALL1600-CC、RG-WALL1600-SC、RG-WALL1600-SI、RG-WALL1600-SA、RG-WALL1600-EI、RG-WALL1600-EA、RG-WALL1600-XI、RG-WALL1600-XA。

WALL 1600-SC 是一款常见的防火墙产品，如图 7-1-1 所示。



图 7-1-1 WALL 1600-SC 示意图

- (1) USB 接口，可以存放日志信息或者加载版本。
- (2) Console 接口，配置设备使用的连接口。
- (3) GE0 接口，管理接口，也可以通过该接口发送数据。
- (4) GE1-5 接口，自协商千兆电口。

2. 产品部署模式

NGFW 有四种工作模式：路由模式、透明模式、旁路模式及混合模式。

- 路由模式：把设备当做网络出口，充分使用设备的 NAT、路由选路、行为控制、VPN 等功能的部署方式，如图 7-1-2 所示。
- 透明模式：当用户网络已具备高性能的网络出口时，若想使用 NGFW 的功能，则可以把 NGFW 串接在内网核心交换机和网络出口设备之间，用户将不必变更网络拓扑和路由，即可使用 NGFW 的行为控制、VPN 等功能，如图 7-1-3 所示。
- 旁路模式：当用户网络已具备高性能的网络出口，也不想把设备串接在内网核心交换机和出口设备之间，又想使用 NGFW 的 VPN、DHCP 等功能时，可将设备像一台服务器一样旁挂在核心交换机上，如图 7-1-4 所示。
- 混合模式：指设备同时工作于路由模式和透明模式，将多个接口配置为一组透明桥，同时此桥组上实现 NAT、路由等功能，如图 7-1-5 所示。



图 7-1-2 路由模式防火墙

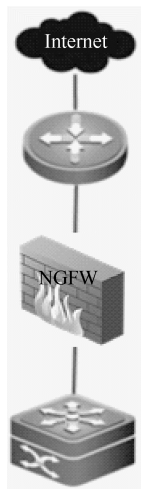


图 7-1-3 透明模式防火墙

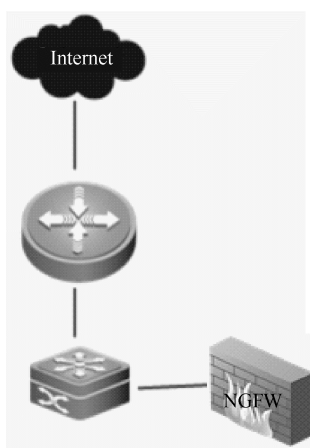


图 7-1-4 旁路模式防火墙

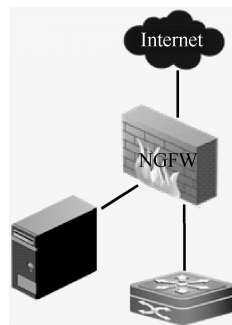


图 7-1-5 混合模式防火墙

3. 管理方式

WALL 1600 下一代防火墙管理方法有 Web 管理和命令行管理。命令行管理包括使用 Console 口管理、Telnet 管理和 SSH 管理等。目前大部分选择使用 Web 方式管理。

(1) 使用 Web 方式管理。

如图 7-1-6 所示, WALL 1600 出厂配置下可以通过接口 GE0 的默认地址 192.168.1.200 进行 Web 管理。将计算机 IP 地址设置为 192.168.1.0/24, 并连接到 GE0 口, 打开 IE 浏览器, 输入 <https://192.168.1.200>, 登录 NGFW 的管理页面, 输入用户名 admin、默认密码 firewall 和验证码, 进入 NGFW 设备首页。

登录设备后可开启其他接口的管理功能。默认其他接口是没有 IP 地址的, 也未开启 HTTPS 等其他管理功能。

详细配置方法如下。

(1) 在 NGFW 出厂配置情况下, 将计算机设置为 192.168.1.1, 网关设置为 192.168.1.200, 如图 7-1-7 所示。

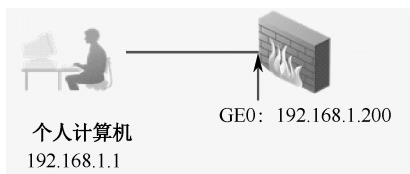


图 7-1-6 防火墙 Web 管理方式

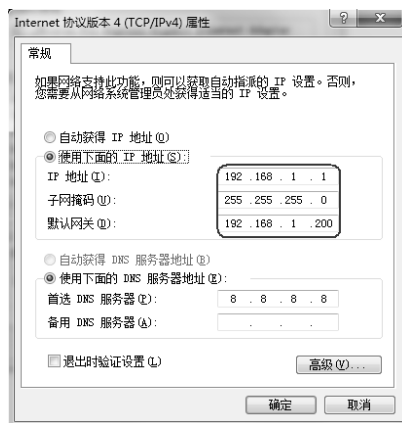


图 7-1-7 使用 Web 管理防火墙 1

(2) 在浏览器里输入 <https://192.168.1.200>, 输入用户名 admin, 密码 firewall 及随机验证码即可进入防火墙首页, 如图 7-1-8 和图 7-1-9 所示。

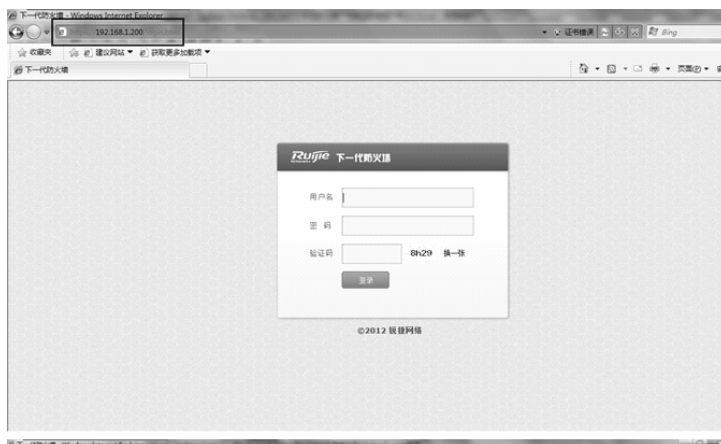


图 7-1-8 使用 Web 管理防火墙 2



图 7-1-9 使用 Web 管理防火墙 3

(3) 配置 ge1 的管理地址为 192.168.33.51/24，并开启 ge1 的管理功能。选择“菜单”“网络管理”“接口”命令编辑 ge1，如图 7-1-10 所示。



图 7-1-10 使用 Web 管理防火墙 4

(4) 配置 ge1 接口 IP 地址为 192.168.33.51/24，在“管理访问”选项组中勾选需开启的功能，如图 7-1-11 所示。



图 7-1-11 使用 Web 管理防火墙 5

- HTTPS: 允许用户以https://192.168.33.51进行管理。
- PING: 允许用户 Ping 此接口地址，如果不勾选此复选框，则在路由可达的情况下也 Ping 不通。
- TELNET: 允许用户用 telnet 192.168.33.51 方式进行管理。

- SSH: 允许用户用 SSH 方式管理设备。
- HTTP: 允许用户用 `http://192.168.33.51` 进行管理。

第五步：验证效果。在浏览器里输入 `https://192.168.33.51`，即可登录管理，如图 7-1-12 所示。



图 7-1-12 使用 Web 管理防火墙 6

2. 使用 Console 进行管理

若需要进入命令行进行配置管理，则可通过 Console 线使用超级终端或 CRT 等软件进入命令行，NGFW 默认允许 Console 管理。NGFW 命令行的命令与锐捷交换机路由器的命令基本类似起来。

如图 7-1-13 所示，将计算机与防火墙连接起来。

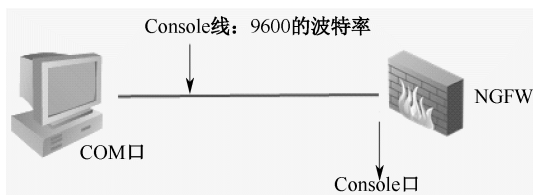


图 7-1-13 Console 方式管理

具体操作方式如下。

- (1) 准备配置线及可连接配置线的计算机。
- (2) 连接配置线，配置线的水晶头端连接到设备的 Console 口上，另一端连接计算机的 COM 口。
- (3) 配置超级终端。
 - Windows XP 系统一般在附件里自带了超级终端，如果是 Windows 7 系统，则需要另外下载超级终端。
 - Windows Server 2003 默认不安装“超级终端”，需在“控制面板”的“添加/删除程序”中进行添加，或直接从“附件一”下载使用。
 - 若设置后无法进入命令行，请检查：配置线是否连接在 Console 口；超级终端的数据位是否配置正确；是否单击还原为默认值。如果以上操作都正确，但是依然无法进入，请尝试更换计算机、配置线及超级终端。
- (4) 验证配置。如图 7-1-14 所示，提示输入用户名 admin 及密码 firewall。

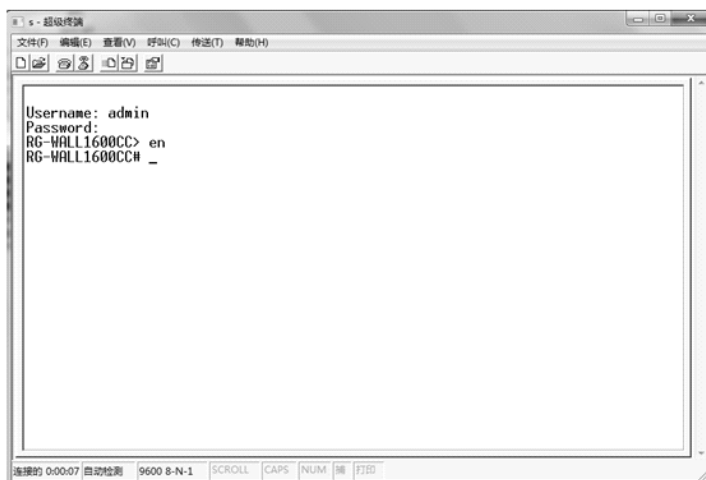


图 7-1-14 Console 登录界面

7.1.2 防火墙初始化配置

1. 页面介绍

如图 7-1-15 所示，菜单提供了 NGFW 设备的主要配置选项。其主要有以下功能。



图 7-1-15 Web 页面示意

- 系统管理：系统配置和管理，包括状态、会话、管理员、维护和监控。
- 网络管理：网络相关配置，包括接口、NAT、基本配置、DHCP、双机热备功能的配置。
- 路由管理：路由相关配置，包括查看路由表、配置路由表、静态路由、策略路由、动态路由和多播路由。
- 资源管理：资源相关配置，包括时间资源、服务资源、地址资源、认证用户及 CA 中心的配置。
- 防火墙：防火墙相关配置，包括安全策略、防 ARP 攻击、Web 认证、MAC 过滤配置。
- VPN：配置 VPN，包括 IPSec、SSL 远程接入、SSL 网关、L2TP VPN 和本地证书的配置。
- 入侵防御：配置入侵防御，包括基于特征的入侵防御、Web 防护。

- 病毒防护：配置防病毒系统，包括文件扫描列表和文件屏蔽列表的配置。
- 应用控制：监控 IM 和 P2P 消息和文件传输，监控流媒体、网络游戏、股票软件。
- 内容过滤：配置 Web 过滤及邮件过滤功能。
- 反垃圾邮件：配置反垃圾邮件功能，包括 IP 地址分析、发件人认证、收件人认证、自定义策略及邮件日志等功能。
- 日志管理：配置和查看日志，包括基本的日志和 NetFlow 配置，以及本地日志的查看。

需要注意的是，很多管理配置页面是列表的形式，如管理员、接口、安全策略等。以安全策略为例，如图 7-1-16 所示。

#	源地址	目的地址	时间表	服务	安全防护	动作	启用
▼ any->any (0/1)							
1	any	any	always	any	<input checked="" type="checkbox"/>	PERMIT	<input type="checkbox"/>
▼ ge1->ge5 (0/1)							
2	any	any	always	any	<input checked="" type="checkbox"/>	PERMIT	<input checked="" type="checkbox"/>

图 7-1-16 防火墙列表示意图

列表中的条目显示项信息。列表中最右面的列一般为可操作提示字段，可对该条目进行一些操作，如编辑、移动、插入、删除等。通过列表上方的“+新建”提示，可以增加条目。单击“+新建”按钮后切换到对话框形式的页面，新建和编辑操作的页面是基本一致的。

2. 默认配置

(1) 接口 0 的默认配置：接口 0 的默认地址配置为 192.168.1.200/24。允许对该接口进行 Ping、HTTPS 操作。

(2) 默认管理员用户：系统默认的管理员用户为 admin，密码为 firewall。用户可以使用这个管理员账号从任何地址登录设备，并且使用设备的所有功能。系统默认的审计员用户为 audit，密码为 audit123。用户可以使用这个账号对安全策略和日志系统进行审计。系统默认的用户管理员用户为 useradmin，密码为 useradmin。用户可以使用这个账号配置系统管理员。

【综合实训】：配置防火墙管理员

网络场景

如图 7-1-17 所示，顶新理工学院有防火墙，需要登录到防火墙上通过修改管理员权限、管理员用户名和密码、管理主机 IP 地址来加强设备管理的安全性。



图 7-1-17 顶新理工学院的防火墙

实施过程

1. 修改 amin 管理员密码

选择“系统管理” “管理员” “管理员”命令，编辑用户名“admin”，如图 7-1-18 所示，输入新密码 ruijie@123，选择“高级”选项，填写管理 IP 地址为 172.18. 10.108/32。



图 7-1-18 防火墙配置管理员信息 1

如果配置为 0.0.0.0/0，则管理 IP 不受限制，任何地址都可以用此账号登录并进行管理，其安全性不高，不建议如此配置，如图 7-1-19 所示。



图 7-1-19 防火墙配置管理员信息 2

2. 配置权限

添加权限类型 test 只有查看和配置日志的权限。选择“系统管理”“管理员”“管理员权限表”“新建”命令进行操作，如图 7-1-20 所示。

3. 设置管理 IP 并添加管理员账号

设置管理 IP 并添加管理员账号 test，配置密码为 123456a!，权限设置为 test，管理主机 IP 不限。选择“系统管理”“管理员”“新建”命令，在“高级”选项处配置管理 IP 为任意，即 0.0.0.0/0，如图 7-1-21 所示。



图 7-1-20 防火墙配置管理员信息 3



图 7-1-21 防火墙配置管理员信息 4

若密码未符合要求，则会出现提示，如图 7-1-22 所示。



4. 配置管理员其他选项

进入“系统配置”“维护”“系统配置”页面，设置页面超时时间为 10 分钟，在线管理员为 10，管理员最大登录重试次数为 5，管理员登录失败阻断间隔为 60 秒，如图 7-1-23 所示。



图 7-1-22 防火墙配置管理员信息 5



图 7-1-23 防火墙配置管理员信息 6

5. 验证效果

(1) 使用 test 账号登录设备，如图 7-1-24 所示。



图 7-1-24 防火墙配置管理员信息 7

(2) 单击除“日志管理”模块的其他功能会提示“登录用户没有操作权限”，且右上角会提示当前使用了哪个账号登录，如图 7-1-25 所示。



图 7-1-25 防火墙配置管理员信息 8

(3) “日志管理”模块可以正常操作，如图 7-1-26 所示。



图 7-1-26 防火墙配置管理员信息 9

【综合实训】：配置防火墙路由模式

网络场景

如图 7-1-27 所示，NGFW 作为网络出口，使用静态地址上网。内网网段为 192.168.1.0/24，内网口 ge0 的 IP 地址设置为 192.168.1.254/24，作为内网网关；外网接口 ge1 的 IP 地址为 192.168.33.51/24，网关为 192.168.33.1。

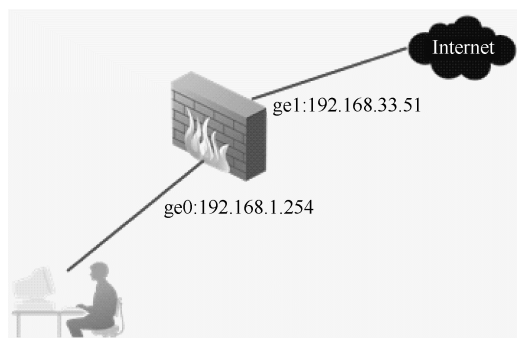


图 7-1-27 防火墙路由模式

实施过程

1. 配置接口地址

(1) 进入“菜单”“网络管理”“接口”“ge0”页面进行编辑，如图 7-1-28 所示。设置 ge0 为 192.168.1.254/24，如图 7-1-29 所示。

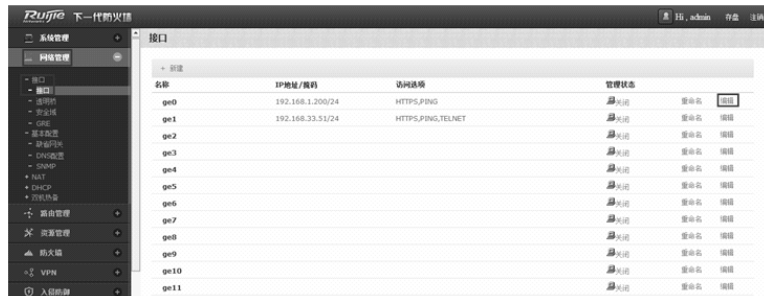


图 7-1-28 防火墙路由模式 1

(2) 进入“菜单”“网络管理”“接口”“ge1”页面进行编辑，如图 7-1-30 所示。配置 ge1 为 192.168.33.51/24，如图 7-1-31 所示。

(3) 配置后查看两个接口的地址，如图 7-1-32 所示。



图 7-1-29 防火墙路由模式 2



图 7-1-30 防火墙路由模式 3



图 7-1-31 防火墙路由模式 4



图 7-1-32 防火墙路由模式 5

2. 配置地址资源

(1) 选择“菜单”“资源管理”“地址资源”“地址结点”“新建”命令，如图 7-1-33 所示。

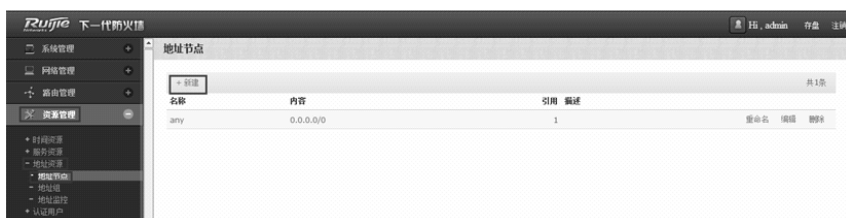


图 7-1-33 防火墙路由模式 6

(2) 名称为“上网网段”，地址结点选择子网“192.168.1.0/24”，单击“提交”按钮，如图 7-1-34 所示。



图 7-1-34 防火墙路由模式 7

3. 配置默认路由

(1) 选择“菜单”“网络管理”“基本配置”“缺省网关”“新建”命令，如图 7-1-35 所示。



图 7-1-35 防火墙路由模式 8



(2) 配置网关地址为 192.168.33.1，如图 7-1-36 所示。

新建缺省网关	
网关地址	192.168.33.1
权重	1 (1-100)
管理距离	1 (1-255)
<input type="button" value="提交"/> <input type="button" value="取消"/>	

图 7-1-36 防火墙路由模式 9

4. 配置 NAT 规则

(1) 进入“菜单”“网络管理”“NAT”“NAT 规则”“新建”页面，如图 7-1-37 所示。

#	源地址	目标地址	服务	出接口	转换后源地址	日志	描述
---	-----	------	----	-----	--------	----	----

图 7-1-37 防火墙路由模式 10

- (2) 源地址选择刚才定义的地地址资源“上网网段”。
- (3) 目的地址选择“any”。
- (4) 服务为“any”。
- (5) 出接口为“ge1”。
- (6) 转换后源地址为“出接口地址”，如图 7-1-38 所示。

5. 配置安全策略

- (1) 选择“菜单”“防火墙”“安全策略”“新建”命令，如图 7-1-39 所示。
- (2) 源接口为 ge0（内网口）。
- (3) 源地址名为刚才定义的“上网网段”。
- (4) 目的接口为 ge1（外网口）。
- (5) 目的地址名为 any。
- (6) 服务为 any。
- (7) 时间表为 always，即所有时间。
- (8) 动作为 permit，如图 7-1-40 所示。

#	源地址	目标地址	服务	出接口	转换后源地址	日志	描述
---	-----	------	----	-----	--------	----	----

图 7-1-38 防火墙路由模式 11



图 7-1-39 防火墙路由模式 12



图 7-1-40 防火墙路由模式 13

配置好安全策略后，必须在全局下选择“菜单”“防火墙”“安全策略”命令，将此策略启用，否则不生效，如图 7-1-41 所示。



图 7-1-41 防火墙路由模式 14

6. 保存配置

保存配置，如图 7-1-42 所示。



图 7-1-42 防火墙路由模式 15

7. 验证效果

将计算机 IP 地址设置为 192.168.1.1/24，网关设置为 192.168.1.254，DNS 配置为 8.8.8.8



（一般设置为当地的 DNS 即可），如图 7-1-43 所示。

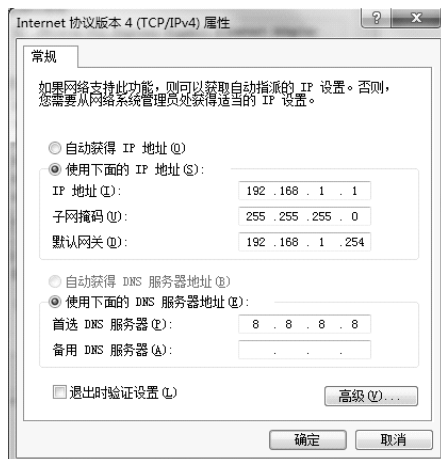


图 7-1-43 防火墙路由模式 16

此时，计算机可正常上网。

任务 2 防火墙安全配置

7.2.1 使用防火墙实现安全 NAT

1. 配置地址池

地址池中存放供动态 NAT 使用的地址范围的集合。地址池的使用支持轮转方式和非轮转方式，也支持地址池分段。在进行地址转换后，报文的真实地址将被转换为地址池中的地址。配置步骤如下。

（1）进入“网络管理”“NAT”“NAT 地址池”页面，单击“新建”按钮，如图 7-2-1 所示。

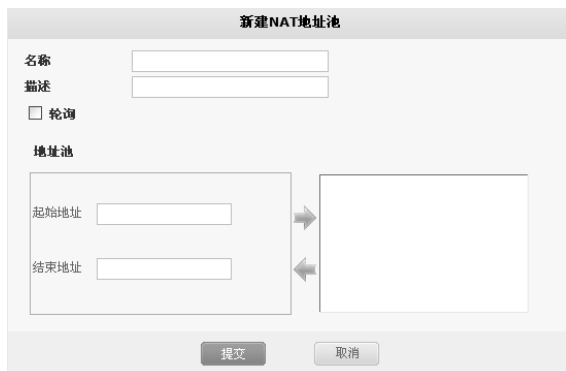


图 7-2-1 创建地址池

- 名称：NAT 地址池的名称，可以是中文。
- 起始地址：NAT 地址池中的起始地址。
- 结束地址：NAT 地址池中的结束地址，结束地址不能小于起始地址。从起始地址到结束地址这个范围内的地址都是地址池中的地址。
- 轮询：地址池中地址数量大于一个时，在进行地址转换的时候会根据从小到大的次序进行循环使用，相同源地址的数据报会分配相同的地址池地址。

需要注意的是，池段范围不能出现重叠现象。

(2) 设置完成后单击“提交”按钮。

2. 配置源地址转换

源地址转换是一种单向的针对源地址的映射，主要用于内网访问外网，减少公有地址的数目，隐藏内部地址。具体配置步骤如下。

(1) 进入“网络管理”“NAT”“NAT 规则”“源地址转换”页面，单击“新建”按钮，如图 7-2-2 所示。

新建源地址转换	
源地址	-----地址-----
目标地址	-----地址-----
服务	-----预定义服务-----
出接口	ge4
转换后源地址	出接口地址
描述	
<input type="checkbox"/> Syslog 日志	
<div>提交</div> <div>取消</div>	

图 7-2-2 新建源地址转换

- 源地址：NAT 规则匹配的源地址，可以是地址结点或地址组。
- 目标地址：NAT 规则匹配的目的地地址，可以是地址结点或地址组。
- 服务：NAT 规则匹配的服务名，可以是服务资源或服务组。
- 出接口：NAT 规则匹配的出接口名。
- 转换后源地址：需要转换成的地址，可以是出接口的地址或地址池名称。
- 描述：对该转换规则的描述。
- Syslog 日志：是否需要对该规则启用日志。

(2) 设置完成后单击“提交”按钮。

3. 配置静态地址转换

静态地址转换是一对一的双向地址映射。在这种情况下，被映射的内部主机可以主动访问外部，外部也可以主动访问这台内部主机，相当于在内、外网之间建立了一条双向通道。具体配置步骤如下。

(1) 进入“网络管理”“NAT”“NAT 规则”“静态地址转换”界面，单击“新建”按钮，如图 7-2-3 所示。



图 7-2-3 创建静态地址转换

- 外部地址：需要转换的外部地址。
- 内部地址：需要转换的内部地址。
- 外部接口：和外部网络相连的接口名。
- 描述：对该转换规则的描述。
- Syslog 日志：是否需要对该规则启用日志。

(2) 配置完成后单击“提交”按钮。

4. 常见问题分析

连接时通时断，配置了 NAT 之后，经过 NAT 后 Ping 其他网络的机器，时通时断；或刚开始是通的，一会儿又断了；或一直不通。这个问题主要有以下两种情况。

(1) 转换后的地址有冲突，别人已经使用。有些地址可能 Ping 不通，但不能排除地址已被使用的可能，因为对方可以禁止了 Ping 包。

(2) 可以查看被 Ping 的机器中的 ARP 表项，NAT 转换后的地址对应的 MAC 是否为设备的 MAC 地址，若不是，证明有其他机器使用了此 IP。使用无人使用的地址作为 NAT 转换后的地址即可。

7.2.2 使用防火墙防止 DoS 攻击和扫描

1. 概述

防 DoS (Denial of Service) 攻击设计的目标就是使设备能够阻止外部的恶意攻击，同时能使内网正常地与外界通信，不仅保护设备，更要保护内网。当遭受到攻击时，向用户进行报警提示。常见的 DoS 攻击主要包括 PING of Death、Tear Drop Attack、Jolt2 Attack、Syn Flood、ICMP Flood、UDP Flood、ARP Flood、SYN Fragment、Land-Base、Winnuke 等。

扫描也是网络攻击的一种，攻击者在发起网络攻击之前，通常会试图确定目标上开放的 TCP/UDP 端口，而一个开放的端口通常意味着某种应用。常见的扫描主要有以下几种。

- 垂直 (Vertical) 扫描：针对相同主机的多个端口。
- 水平 (Horizontal) 扫描：针对多个主机的相同端口。
- ICMP (PING) sweeps：针对某地址范围，通过 Ping 方式发现存活主机。

NGFW 设备可以有效防范以上几类扫描，从而阻止外部的恶意攻击，保护设备和内网。当检测到此类扫描探测时，向用户进行报警提示。

2. 配置

(1) 进入“入侵防御”“防攻击”“配置”页面并进行操作，如图 7-2-4 所示。

防 DOS 攻击的相关配置如下。

- Jolt2: Jolt2 攻击通过向目的主机发送报文偏移加上报文长度超过 65535 的报文，使目的主机处理异常而崩溃。配置了防 Jolt2 攻击功能后，NGFW 可以检测出 Jolt2 攻击，丢弃攻击报文并输出告警日志信息。
- Land-Base: Land-Base 攻击通过向目的主机发送目的地址和源地址相同的报文，使目的主机消耗大量的系统资源，从而造成系统崩溃或死机。配置了防 Land-Base 攻击功能后，NGFW 可以检测出 Land-Base 攻击，丢弃攻击报文并输出告警日志信息。
- PING of death: PING of death 攻击通过向目的主机发送长度超过 65535 的 ICMP 报文，使目的主机发生处理异常而崩溃。配置了防 PING of death 攻击功能后，NGFW 可以检测出 PING of death 攻击，丢弃攻击报文并输出告警日志信息。
- Syn flag: Syn-flag 攻击通过向目的主机发送错误的 TCP 标识组合报文，浪费目的主机资源。配置了防 Syn-flag 攻击功能后，NGFW 可以检测出 Syn-flag 攻击，丢弃攻击报文并输出告警日志信息。
- Tear drop: Tear-drop 攻击通过向目的主机发送报文偏移重叠的分片报文，使目的主机发生处理异常而崩溃。配置了防 Tear-drop 攻击功能后，NGFW 可以检测出 Tear-drop 攻击，并输出告警日志信息。因为正常报文传送也有可能出现报文重叠，因此 NGFW 不会丢弃该报文，而是采取裁减、重新组装报文的方式，发送出正常的报文。
- Winnuke: Winnuke 攻击通过向目的主机的 139、138、137、113、53 端口发送 TCP 紧急标识位为 1 的带外数据报文，使系统处理异常而崩溃。配置了防 Winnuke 攻击功能后，NGFW 可以检测出 Winnuke 攻击报文，将报文中的 TCP 紧急标志位为 0 后转发报文，并可以输出告警日志信息。
- Smurf: 这种攻击方法结合使用了 IP 欺骗和 ICMP 回复方法使大量网络传输充斥目的系统，使得目的系统拒绝为正常系统进行服务。Smurf 攻击通过使用将回复地址设置成受害网络的广播地址的 ICMP 应答请求 (PING) 数据包，来淹没受害主机，最终导致该网络的所有主机都对此 ICMP 应答请求做出答复，导致网络阻塞。

图 7-2-4 防 DOS 和防扫描配置



防扫描的相关配置如下。

- TCP 协议扫描：根据实际网络情况，当受到 TCP 扫描攻击时，可以配置防 TCP 扫描。当一个源 IP 地址在 1 秒内将含有 TCP SYN 片段的 IP 封包发送给位于相同目的 IP 地址的不同端口数量大于配置的门限值时，即认为其进行了端口扫描，系统将其标记为 TCP SCAN，并在配置的阻断时间内拒绝来自于该源主机的所有其他 TCP SYN 包。启用防 TCP 扫描，可能会占用比较多的内存。
- UDP 协议扫描，根据实际网络情况，当受到 UDP 扫描攻击时，可以配置防 UDP SCAN 扫描。当一个源 IP 地址在 1 秒内将含有 UDP 的 IP 封包发送给位于相同目的 IP 地址的不同端口数量大于配置的门限值时，即进行了一次端口扫描，系统将其标记为 UDP SCAN，并在配置的阻断时间内拒绝来自于该源主机的所有其他 UDP 包。启用防 UDP 扫描，可能会占用比较多的内存。
- PING 扫描：根据实际网络情况，当受到 PING 扫描攻击时，可以配置防 PING 扫描。当一个源 IP 地址在 1 秒内发送给不同主机的 ICMP 封包超过门限值时，即进行了一次地址扫描。此方案的目的是将 ICMP 封包（通常是应答请求）发送给各个主机，以期获得至少一个回复，从而查明目的地址。NGFW 设备在内部记录从某一远程源地点发往不同地址的 ICMP 封包数目。当某个源 IP 被标记为地址扫描攻击时，系统在配置的阻断时间内拒绝来自该主机的其他更多 ICMP 封包。启用防 PING 扫描，可能会占用比较多的内存。
- 主机抑制时长：设置防扫描功能的阻断时间，当系统检测到扫描攻击时，在配置的时长内拒绝来自于该源主机的所有其他攻击包，默认配置为 20 秒。
- 扫描识别阈值：防扫描功能的扫描识别门限，超过阈值时，该源 IP 被标记为扫描攻击，来自于该源主机的所有其他攻击包都被阻断，默认配置为 100。

智能 FLOOD 防御 TCP Flood

TCP Flood 即 SYN Flood 攻击，是众多 DoS 攻击形式的一种方式。SYN Flood 利用 TCP 协议的缺陷，向服务器端发送大量伪造的 TCP 连接请求之后，自身不再做出应答，使得服务器端的资源迅速耗尽，从而无法及时处理其他正常的服务请求，严重时甚至会导致服务器系统崩溃。NGFW 的防 SYN Flood 攻击采用了业界最新的 Syncookie 技术，在很少占用系统资源的情况下，可以有效地抵御 SYN Flood 对受保护服务器的攻击。

- 识别门限：配置 TCP 半连接的阈值，即防 TCP Flood 攻击的启动门限，默认配置为 300。

(2) 按照需要启用防攻击相关功能，并输入合法参数。

(3) 配置完成后，单击“提交”按钮。

7.2.3 配置防火墙用户地址绑定

1. 安全策略概述

为了对数据流进行统一控制，方便用户配置和管理，NGFW 设备引入了安全策略的概念。通过配置安全策略，防火墙能够对经过设备的数据流进行有效的控制和管理。当防火墙收到数据报文时，对该报文的方向、源地址、目的地址、协议、端口等信息和用户配置的策略进行匹配，决定是否建立这条数据流，并且把这条流和匹配的策略关联起来，从而确定如何处理该流的后续报文，实现允许、丢弃、加密和解密、认证、排定优先次序、调度、过滤及监控数据流，决定哪些用户和数据能进出，以及它们进出的时间和地点。

同时，在安全策略中还可以根据匹配结果，对符合规则的报文实行过滤动作（允许通过

或丢弃)，简单地实现包过滤功能。在没有配置任何安全策略的情况下，对于经过设备的所有数据包，其默认策略为“禁止”。安全策略按先配置先匹配的原则，只对通过设备的数据包进行处理，对于到设备本身的数据包和设备本身发出的数据包不进行限制。

安全策略的基本要素是匹配条件和动作。匹配条件包括数据流的方向、源地址、目的地址、服务和策略生效的时间范围。

其中，数据流的方向通过指定入接口/安全域和出接口/安全域来确定，源地址、目的地址、服务和时间范围都可以直接引用已定义的对象。策略的动作有 PERMIT、DENY，IPSEC、SSL-VPN。不同的动作下又有不同的可选配置，从而决定对符合匹配条件的数据流实现哪些业务。

2. 配置

(1) 进入“防火墙” “安全策略” “安全策略”页面，单击“新建”按钮，如图 7-2-5 所示。

新建安全策略

源

接口/安全域 any

地址名 any

目的

接口/安全域 any

地址名 any

服务 any

时间表 always

动作 PERMIT

☐ 安全防护

☐ 流量日志

高级选项>>

描述

提交 取消

图 7-2-5 防火墙安全策略 1

- 源的接口/安全域：数据流的流入方向，可以指定某个接口，也可以是已定义的某个安全域，any 表示所有接口。
- 源的地址名：数据流的源地址，可以引用已定义的某个地址结点或地址结点组，any 表示源地址为任意。
- 目的的接口/安全域：数据流的流出方向，可以指定某个接口，也可以是已定义的某个安全域，any 表示所有接口。
- 目的的地址名：数据流的目的地址，可以引用已定义的某个地址结点或地址结点组，any 表示目的地址为任意。
- 服务：数据流的服务属性，包括协议、源端口和目的端口，可以引用系统预定义服务、已定义的服务资源或服务资源组，any 表示服务为任意。
- 时间表：策略生效的时间，可以引用已配置的时间资源，always 表示所有时间。
- 动作：对符合匹配条件的数据流执行的动作，PERMIT 为允许，DENY 为拒绝，IPSEC 为 IPSec 加密，SSL-VPN 为 SSLVPN 加密。
- 描述：安全策略的描述，长度限制为 127 个字符。



(2) 设置完成后单击“提交”按钮。

需要注意的是，创建一条新的安全策略时，系统会自动生成该策略的 ID，策略 ID 是安全策略的唯一标识。

(3) 启用安全策略。

配置好的安全策略必须启用才能使其生效。配置步骤如下。

进入“防火墙”“安全策略”页面，如图 7-2-6 所示。



图 7-2-6 防火墙安全策略 2

勾选“启用”复选框，可以启用一条策略。

需要注意，安全策略默认为不启用，配置后必须手工启用才能使其生效。

7.2.4 使用防火墙限制连接带宽

1. 概述

要对用户带宽进行限制，要先针对需要限制的用户地址段，定义相应的地址对象。在安全策略里调用之前的用户地址段，设置高级选项中的“流量控制”。

需要注意，在流量控制中，可以设置“优先级”，该优先级表示数据优先转发的级别。策略上行/下行针对的是整个网段，主机上行/下行针对的是每个 IP 用户。

2. 配置

(1) 针对需要限制的用户地址段，定义相应的地址对象，如图 7-2-7 所示。



图 7-2-7 限制用户带宽 1

(2) 在安全策略里调用之前的用户地址段，设置高级选项中的“流量控制”，如图 7-2-8 所示。



图 7-2-8 限制用户带宽 2

选择“高级选项”选项，如图 7-2-9 所示。



图 7-2-9 限制用户带宽 3

单击“提交”按钮，如图 7-2-10 所示。



图 7-2-10 限制用户带宽 4

- 流量控制：启用流量控制功能，对策略中指定的流进行服务质量保证。
- 在优先级设置中设定数据流的优先级，优先级从高到低有 High、Medium、Normal、Low 四种，默认为 Normal，匹配该策略的流根据此优先级转发。
- 在策略上/下行带宽限制中设定最大带宽，取值为 10~10000000kb/s，为空时表示不限速。
- 配置流量限速值后匹配该策略的流上/下行方向最大带宽不超过相应限速值。



➤ 策略上行针对的是整个网段，主机上行针对的是每个 IP 用户。

7.2.5 使用防火墙实现 URL 过滤

1. 概述

Web 过滤模块针对 HTTP 协议为用户提供应用级的安全防护和访问限制。Web 过滤大致分为两个方面：一方面是对 HTTP 请求的过滤，主要是对 URL 的过滤；另一方面是对 HTTP 响应的过滤，主要是对 HTTP 内容的过滤。

NGFW 设备中 URL 过滤的基本过程如下：首先在 URL 列表中添加模式字符串，然后在安全防护表模板中启用 Web 过滤功能并选择 URL 列表类型，最后在策略中引用该安全防护表模板并启用策略。

系统中有屏蔽和免屏蔽两个 URL 列表，每个列表中可以添加多个模式字符串。屏蔽列表的过滤行为是 deny，即匹配上该列表中的模式字符串的流要被过滤掉，否则放行；免屏蔽列表的过滤行为是 accept，即匹配上该列表中的模式字符串的流可以通过，否则被过滤。对于用户的 URL 请求，先查找 URL 中是否包含列表中的模式字符串，从而执行列表的过滤规则。

关键字过滤：关键字过滤是一套功能强大且容易使用的内容监控系统。一直以来，由于一些不法分子利用网络来传播一些色情、反动等非法信息，这些非法信息会给人们的精神生活带来不利的影响。NGFW 的关键字过滤主要是针对网页内容文字的过滤。控制用户对非法内容的访问，管理员能够通过页面配置被禁止的文字。本模块仅支持 GB2312、UTF-8 编码的中文，最多支持 3 个“与”关系。

内容过滤：随着 Internet 的迅猛发展，网页的内容日益丰富，各种网页控件的应用越来越被广泛，不仅占用网络及系统资源，而且给互联网以及使用者带来了很大的安全隐患。NGFW 设备能够对 Java Applet、Cookie、Script、Object 控件进行过滤，保证上网者安全使用网络。

Web 代理阻止：指当客户在浏览器中设置好 Proxy Server 后，使用浏览器访问所有 WWW 站点的请求都不会直接发给目的主机，而是先发给代理服务器，代理服务器接受了客户的请求以后，由代理服务器向目的主机发出请求，并接收目的主机的数据，在 NGFW 中具有禁止 HTTP 代理的功能。

2. 配置

(1) 配置 URL 屏蔽列表。

在 URL 屏蔽列表中添加模式字符串，URL 中包含这些模式字符串的 HTTP 请求会被过滤掉。配置步骤如下。

进入“Web 过滤” “屏蔽列表”页面，如图 7-2-11 所示。

屏蔽URL列表	<input type="checkbox"/> 启用	
test	<input checked="" type="checkbox"/>	删除

图 7-2-11 配置 Web 过滤 1

在输入框中输入模式字符串。

- 新建：添加一个模式字符串到 URL 屏蔽列表中。
- 启用：使模式字符串生效，模式字符串的默认状态为不启用。
- 删除：从 URL 屏蔽列表中删除一个模式字符串。
- 清空所有：从 URL 屏蔽列表中删除所有模式字符串。

单击“提交”按钮，使当前 URL 屏蔽列表的配置生效。

需要注意，单击“提交”按钮后当前 URL 屏蔽列表的配置才能生效；如果一个模式字符串没有启用，则包含该模式串的 URL 请求不会被过滤。

(2) 配置 URL 免屏蔽模板。

在 URL 免屏蔽列表中添加模式字符串，URL 中包含这些模式字符串的请求被允许通过。配置步骤如下。

进入“防火墙 Web 过滤” “免屏蔽列表”页面，如图 7-2-12 所示。

图 7-2-12 配置 Web 过滤 2

在输入框中输入模式字符串。

- 新建：添加一个模式字符串到 URL 免屏蔽列表中。
- 启用：使模式字符串生效，模式字符串的默认状态为不启用。
- 删除：从 URL 免屏蔽列表中删除一个模式字符串。
- 清空所有：从 URL 免屏蔽列表中删除所有模式字符串。

单击“提交”按钮，使当前 URL 免屏蔽列表的配置生效。

需要注意，单击“提交”按钮后当前 URL 免屏蔽列表的配置才能生效。如果一个模式字符串没有启用，则包含该模式串的 URL 请求不会被放行。

(3) 启用关键字过滤。

启用网页内容过滤，进入“防火墙” “安全策略” “安全防护表” “Web 过滤”页面，如图 7-2-13 所示。

图 7-2-13 配置 Web 过滤 3



勾选“关键字过滤”复选框启用此功能。单击“提交”按钮完成配置。

(4) 配置关键字过滤。

进入“应用过滤” “Web 过滤” “关键字过滤”页面，如图 7-2-14 所示。

图 7-2-14 配置 Web 过滤 4

可以增加禁止语句同时支持“与”的关系，如图 7-2-15 所示。

图 7-2-15 配置 Web 过滤 5

单击“提交”按钮完成配置。

(5) 启用网页内容过滤。

进入“防火墙” “安全策略” “安全防护表” “Web 过滤”页面，如图 7-2-16 所示。

勾选“内容过滤”复选框启用此功能。

单击“提交”按钮完成配置。

(6) 配置网页内容过滤各选项。

进入“应用过滤” “Web 过滤” “内容过滤”页面，如图 7-2-17 所示。

图 7-2-16 配置 Web 过滤 6

图 7-2-17 配置 Web 过滤 7

勾选需要的功能的复选框。

单击“提交”按钮完成配置。

(7) 启用禁止 HTTP 代理过滤

进入“防火墙”“安全策略”“安全防护表”“Web 过滤”页面，如图 7-2-18 所示。

勾选“禁止 HTTP 代理”复选框启用此功能。

单击“提交”按钮完成配置。

图 7-2-18 配置 Web 过滤 8

7.2.6 使用防火墙限制 P2P 流量

1. 概述

防火墙配置思路为先新建 P2P 限制模板，限制每个 IP 地址的 P2P 流量的上行和下行；然后新建安全防护列表，调用之前的模板；最后编辑安全策略，调用之前的安全防护列表。单击“存盘”按钮保存配置，否则下次设备重启后配置就丢失了。

2. 配置

(1) 新建 P2P 限制模板，如图 7-2-19 所示。



图 7-2-19 限制 P2P 流量 1

配置好后的效果如图 7-2-20 所示。



图 7-2-20 限制 P2P 流量 2

(2) 新建安全防护列表，调用之前的模板，如图 7-2-21 所示。



图 7-2-21 限制 P2P 流量 3

(3) 编辑安全策略，调用之前的安全防护列表，如图 7-2-22 所示。



图 7-2-22 限制 P2P 流量 4

最终的安全策略如图 7-2-23 所示，务必勾选“启用”复选框，否则配置不会生效。



图 7-2-23 限制 P2P 流量 5

也可以不进行阻断而是限速，在“应用控制”“P2P”“监视器”中可以看到限速后主机的当前速率，如图 7-2-24 所示。

地址名	应用程序	限速(Kbps)
192.168.1.4	酷狗	50

图 7-2-24 限制 P2P 流量 6

(4) 单击“存盘”按钮保存配置，否则下次设备重启后配置就丢失了，如图 7-2-25 所示。



图 7-2-25 限制 P2P 流量 7

需要注意的是，NGFW 的入侵防御、防病毒、应用控制三个功能需要有相应特征库才能使用，NGFW 出厂已有当前最新的特征库版本，但要想让此功能效果理想，需要实时更新特征库的版本，若没有购买正式授权，则特征库无法更新，功能将会不理想；若有授权，并将 License 导入设备，则系统会自动更新到最新版本。

7.2.7 配置防火墙链路负载

1. 概述

有些网络有两条或多条外网线路，如一条电信、一条联通，通过配置实现内网访问电信地址时通过电信线路，访问联通地址时通过网通线路，同时起到冗余备份的作用。

要想实现这样的功能，就必须把电信和网通的明细静态路由全部配置到设备里，可事先



将配置命令在记事本里写好，然后将其复制粘贴到设备里。如果后期发现有走错线的，可以在 Web 上手动添加正确的静态路由。同时，配置各自的默认路由，在其中一条线断开时，可将流量切换到另一条上，起到冗余备份作用。

2. 配置

(1) 配置接口 IP。

进入“菜单”“网络管理”“接口”“编辑”页面，如图 7-2-26 所示。



图 7-2-26 配置防火墙链路负载 1

配置联通接口 IP 地址，如图 7-2-27 所示。



图 7-2-27 配置防火墙链路负载 2

配置电信接口 IP 地址，如图 7-2-28 所示。



图 7-2-28 配置防火墙链路负载 3

配置内网口 IP 地址，如图 7-2-29 所示。



图 7-2-29 配置防火墙链路负载 4

(2) 配置路由。

配置默认路由，进入“菜单”“网络管理”“基本配置”“缺省网关”“新建”页面，如图 7-2-30 所示。



图 7-2-30 配置防火墙链路负载 5

配置电信默认路由，如图 7-2-31 所示。



图 7-2-31 配置防火墙链路负载 6

配置联通默认路由，如图 7-2-32 所示。

配置静态路由。

将电信、联通路由表里的下一跳地址修改为相应的电信和网通网关，然后进入命令行，将路由复制进去，如图 7-2-33 所示。



图 7-2-32 配置防火墙链路负载 7

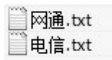


图 7-2-33 配置防火墙链路负载 8



进入防火墙的命令行，把电信和网通的路由表复制进去。

```
Username: admin
Password:
RG-WALL1600CC> en
RG-WALL1600CC# con t
RG-WALL1600CC(config)#ip route 1.0.1.0/24 192.168.33.1
```

(3) 配置 NAT 规则。

配置 NAT 地址池，如图 7-2-34 所示。



图 7-2-34 配置防火墙链路负载 9

配置 NAT 转换规则，如图 7-2-35 所示。

配置电信 NAT 转换，如图 7-2-36 所示。



图 7-2-35 配置防火墙链路负载 10



图 7-2-36 配置防火墙链路负载 11

配置网通 NAT 转换，如图 7-2-37 所示。



图 7-2-37 配置防火墙链路负载 12

(4) 配置安全策略。

具体配置如图 7-2-38 所示。



图 7-2-38 配置防火墙链路负载 13

配置内网通过电信上网，如图 7-2-39 所示。

配置内网通过网通上网，如图 7-2-40 所示。

需要注意配置完策略后务必启用此策略，才会生效，如图 7-2-41 所示。

(5) 保存配置。

保存配置，如图 7-2-42 所示。



安全策略

编辑安全策略

源

接口/安全域: ge4

地址名: 本地网段

目的

接口/安全域: ge2

地址名: any

服务: any

时间表: always

动作: PERMIT

☐ 安全防护

☐ 流量日志

高级选项>>

描述

提交 取消

图 7-2-39 配置防火墙链路负载 14

编辑安全策略

源

接口/安全域: ge4

地址名: any

目的

接口/安全域: ge3

地址名: any

服务: any

时间表: always

动作: PERMIT

☐ 安全防护

☐ 流量日志

高级选项>>

描述

提交 取消

图 7-2-40 配置防火墙链路负载 15

安全策略

源	目的	服务	动作	过虑	共2条
# 源地址	目的地址	时间表	服务	安全防护	动作 启用
▼ ge4->ge2 (1/1)					
1 本地网段	any	always	any		PERMIT <input checked="" type="checkbox"/> 编辑 移动 插入 删除
▼ ge4->ge3 (1/1)					
2 本地网段	any	always	any		PERMIT <input checked="" type="checkbox"/> 编辑 移动 插入 删除

图 7-2-41 配置防火墙链路负载 16



图 7-2-42 配置防火墙链路负载 17

【综合实训】：配置防火墙安全技术

网络场景

如图 7-2-43 所示，将 ge0、ge1 组成一组透明桥，桥组名称为“混合模式”，桥管理地址为 172.18.10.108；配置 ge2 接口 IP 地址为 192.168.100.1，作为内网 PC 的网关；内网 192.168.100.0/24 网段的 PC 通过 NAT 转换为 172.18.10.108 进行上网；服务器地址为 172.18.10.109，网关为 172.18.10.1，无需 NAT 转换直接上网。

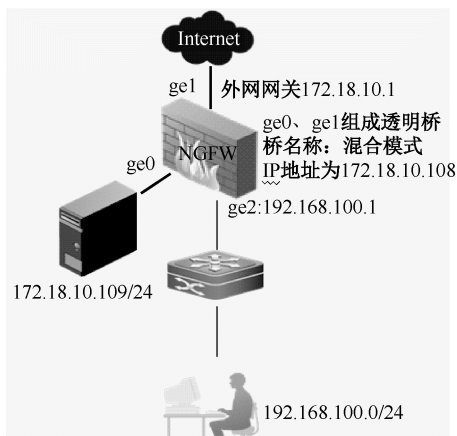


图 7-2-43 防火墙示意图

配置过程

- (1) 新建透明桥：透明桥上配置 IP 地址为 172.18.10.108/24。
- (2) 新建地址结点：分别创建地址结点名 172.18.10.109 和 192.168.100.0。
- (3) 新建 NAT 地址池。
- (4) 配置 NAT 地址转换。
- (5) 配置默认路由。
- (6) 配置安全策略：分别配置内网用户访问外网安全策略、服务器访问外网安全策略。

实施过程

1. 新建透明桥

透明桥上配置 IP 地址为 172.18.10.108/24，如图 7-2-44 所示。



图 7-2-44 防火墙安全 1

配置 ge2 接口地址，如图 7-2-45 所示。



图 7-2-45 防火墙安全 2

2. 新建地址结点

分别创建地址结点名 172.18.10.109 和 192.168.100.0，如图 7-2-46 所示。



图 7-2-46 防火墙安全 3

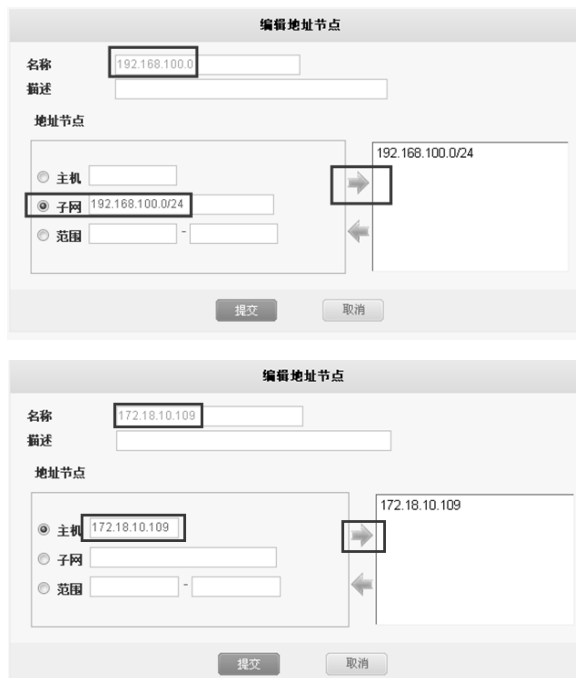


图 7-2-46 防火墙安全 3 (续图)

3. 新建 NAT 地址池

新建 NAT 地址池，如图 7-2-47 所示。



图 7-2-47 防火墙安全 4

4. 配置 NAT 地址转换

配置 NAT 地址转换，如图 7-2-48 所示。



图 7-2-48 防火墙安全 5

5. 配置默认路由

配置默认路由，如图 7-2-49 所示。



图 7-2-49 防火墙安全 6

6. 配置安全策略

配置安全策略，如图 7-2-50 所示。



图 7-2-50 防火墙安全 7

内网 192.168.100.0 网段计算机能访问外网，也可以访问服务器，如图 7-2-51 所示。

内网服务器能访问外网，如图 7-2-52 所示。

需要注意的是，配置安全策略后务必勾选“启用”复选框，如图 7-2-53 所示。

图 7-2-51 防火墙安全 8

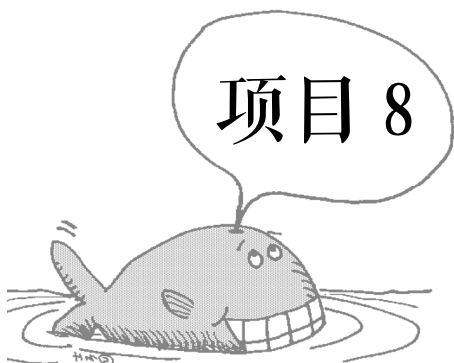
图 7-2-52 防火墙安全 9

安全策略							
+ 新建	源 any	目的 any	服务 any	动作 PERMIT			
#	源地址	目的地址	时间表	服务	安全防护	动作	启用
▼ 混合模式->混合模式 (2/2)							
1	192.168.100.0	any	always	any		PERMIT	<input checked="" type="checkbox"/>
2	172.18.10.109	any	always	any		PERMIT	<input checked="" type="checkbox"/>

图 7-2-53 防火墙安全 10

5. 验证效果

服务器与 PC 均可以正常上网，且内网计算机能访问服务器。



配置无线局域网设备

任务 1 组建 Ad-Hoc 模式无线局域网

8.1.1 无线局域网基础知识

1. 无线局域网

无线网络是计算机网络技术与无线通信技术结合的产物，与有线网络的安装和通信过程一样，只是无线网络利用无线电波信号作为信息的传输媒介，如图 8-1-1 所示。

对于无线局域网（Wireless Local Area Network，WLAN）的定义，有很多种说法。我们先从字面上理解“无线局域网”，可以看出它包含了“无线”和“局域网”两个方面的涵义。

其中，“无线”定义了网络连接的方式，这种连接方式省去了有线局域网中的传输线缆，而利用红外线、微波等无线技术进行信息传输。有线网络的传输媒介主要依赖铜缆或光缆。在某些场合下，有线网络的布线要受环境条件的限制：工程量大；费用昂贵、耗时多；线路容易损坏；网络中的各结点不易移动；网络的扩展受到限制。而无线网络“无线”的特点，正好弥补了以上有线网络的安装和建设中的不足。

“局域网”定义了网络应用的范围，它是将小区域内的各种通信设备互连在一起的通信网络，这个区域可以是一个房间、一个建筑物内，也可以是一个校园的广大区域。

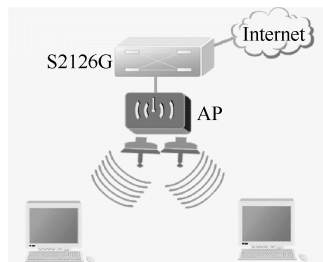


图 8-1-1 无线局域网

2. WLAN 的技术优势

WLAN 是以无线信道作为传输媒介的计算机局域网，是计算机网络与无线通信技术相结合的产物。它以无线多址信道作为传输媒介，提供传统有线局域网的功能，能够使用户实现随时、随地、随意的宽带网络接入，如图 8-1-1 所示。

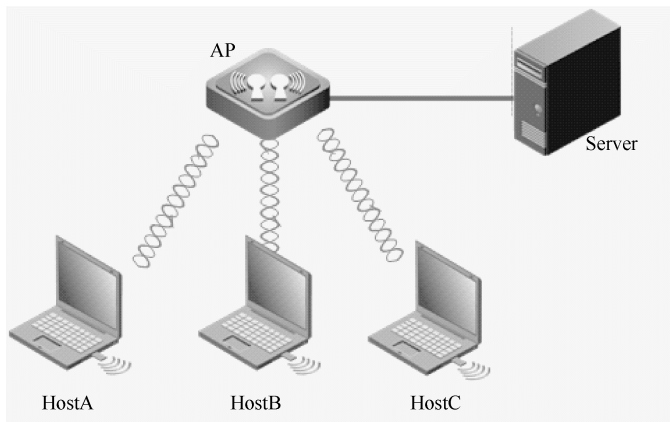


图 8-1-2 无线局域网

WLAN 利用电磁波在空气中发送和接收数据，而无需线缆介质。与有线网络相比，WLAN 具有以下优点。

安装便捷：WLAN 的安装工作简单，不需要布线或开挖沟槽。相比有线网络的安装时间，WLAN 的安装时间少得多。

覆盖范围广：在有线网络中，网络设备的安放位置受网络信息点位置的限制。而无线局域网的通信范围不受环境条件的限制，网络的传输范围大大拓宽了，最大传输范围可达到几十千米。

经济节约：由于有线网络缺少灵活性，这就要求网络规划者尽可能地考虑未来发展的需要，所以往往导致预设大量利用率较低的信息点。而一旦网络的发展超出了设计规划，又要花费较多费用进行网络改造。WLAN 不受布线接点位置的限制，具有传统局域网无法比拟的灵活性，可以避免或减少以上情况的发生。

易于扩展：WLAN 有多种配置方式，能够根据需要灵活选择。这样，WLAN 就能胜任从只有几个用户的小型网络到上千用户的大型网络，并且能够提供类似“漫游”等有线网络无法提供的特性。

传输速率高：WLAN 的数据传输速率现在已经能够与以太网相媲美，而且传输距离可远至 20km 以上。

由于 WLAN 具有多方面的优点，故其发展十分迅速。在最近几年里，WLAN 已经在医院、商店、工厂和学校等不适合网络布线的场合得到了广泛的应用。

3. WLAN 的传输介质

无线信号是能够在空气中进行传播的电磁波，无线信号不需要任何物理介质，它在真空环境中也能够传输，就如同在办公室大楼的空气中传播一样。无线电波不仅能够穿透墙体，还能够覆盖比较大的范围，所以无线技术成为了一种组建网络的通用方法。图8-1-3 展示了电磁波。

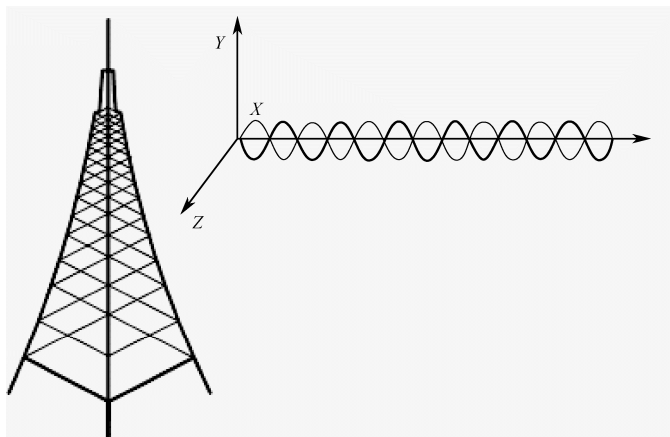


图 8-1-3 电磁波中的编码信号

频谱就是频率的分布曲线，复杂振荡分解为振幅不同和频率不同的谐振荡，这些谐振荡的幅值按频率排列的图形称为频谱，其广泛应用在声学、光学和无线电技术等方面。图 8-1-4 展示了无线频谱图。

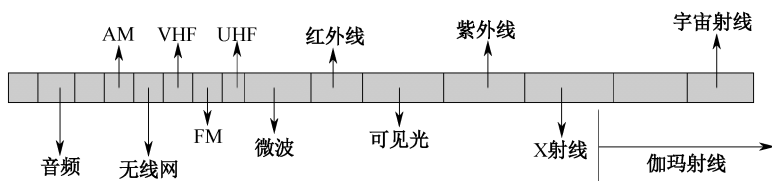


图 8-1-4 无线频谱

WLAN 运行在 2.4~2.4835GHz 的微波频段上，所有的波都以光速传播，这个速度可以被精确地称为电磁波速度。所有的波都遵守公式：频率×波长 = 光速。

各种电磁波之间的主要区别就是频率。如果电磁波频率低，那么它的波长就长；如果电磁波的频率高，那么它的波长就短。波长表示正弦波的两个相邻波峰之间的距离。

8.1.2 组建 WLAN 的网络组件

WLAN 可独立存在，也可与有线局域网共同存在并进行互连。在 WLAN 中最常见的组件如下：笔记本式计算机和 workstation、无线网卡、无线接入点（Access Point，AP）和天线设备。

1. 无线工作站

笔记本式计算机、掌上电脑、个人数字助理和其他小型计算设备正变得越来越普及，都是无线网络中的工作站，作为无线网络的终端接入到网络中。笔记本式计算机和台式机最主要的区别是笔记本式计算机的组件体积小，而且用 PCMCIA（个人计算机存储卡国际协会）插槽取代了扩展槽，从而可以接入无线网卡、调制解调器及其他设备。

目前很多笔记本式计算机和 PDA 都预装了无线网卡，可以直接与其他无线产品或者其他符合 Wi-Fi 标准的设备进行交互。



图 8-1-5 PCMCIA 接口网卡

2. 无线网卡

无线网卡作为无线网络的接口，实现与无线网络的连接，作用类似于有线网络中的以太网网卡。无线网卡根据接口类型的不同，主要分为三种类型，即 PCMCIA 无线网卡、PCI 无线网卡和 USB 无线网卡，如图 8-1-6 和图 8-1-7 所示。



图 8-1-6 PCI 无线网卡



图 8-1-7 USB 无线网卡

PCMCIA 无线网卡仅适用于笔记本式计算机，支持热插拔，可以非常方便地实现移动式无线接入。PCI 无线网卡适用于台式计算机，安装起来相对要复杂一些。USB 无线网卡适用于笔记本式计算机和台式机，支持热插拔，而且安装简单，即插即用。目前 USB 接口的无线网卡得到了大量用户的青睐。

无线网卡的主要功能就是通过无线设备透明地传输数据包，工作在 OSI 参考模型的第 1 层和第 2 层。除了用无线连接取代线缆之外，这些适配器就像标准的网络适配器那样工作，不需要其他特别的无线网络功能。

3. 无线接入点

无线 AP 也称为无线网桥，它的作用是提供无线终端的接入功能，类似于以太网中的集线器，与集线器不同的是，无线 AP 与计算机之间的连接是通过无线信号方式实现的。

无线 AP 是无线网和有线网之间沟通的桥梁，在无线 AP 覆盖范围内的无线工作站通过无线 AP 进行相互之间的通信。无线 AP 的覆盖范围是一个向外扩散的圆形区域，尽量把无线 AP 放置在无线网络的中心，而且各无线客户端与无线 AP 的直线距离最好不要太长，以避免因通信信号衰减过多，而导致通信失败。

当网络中增加一个无线 AP 之后，即可成倍地扩展网络覆盖直径。另外，也可使网络中容纳更多的网络设备。通常情况下，一个 AP 最多可以支持多达 30 台计算机接入，推荐数量为 25 台以下，如图 8-1-8 所示。

无线 AP 基本上都拥有一个以太网接口，用于实现与有线网络的连接，从而使无线终端能够访问有线网络或 Internet 的资源。无线 AP 主要用于宽带家庭、大楼内部及园区内部，典型距离覆盖几十米至上百米。大多数无线 AP 还带有接入点客户端（AP Client）模式，可以和其他 AP 进行无线连接，延展网络的覆盖范围。



图 8-1-8 RG-WG54P 室内型无线 AP

单纯性无线 AP 就是一个无线的交换机，仅提供无线信号发射的功能。单纯性无线 AP 的工作原理是将网络信号通过双绞线传送过来，经过 AP 产品的编译，将电信号转换为无线电信号发送出去。根据不同的功率，可以实现不同程度、不同范围的网络覆盖，一般无线 AP 的最大覆盖距离可达 300m。此外，一些 AP 还具有高级的功能以实现网络接入控制，如 MAC 地址过滤、DHCP 服务器等。



4. 天线控制器 AC

无线控制器（Access Control，AC）是一个无线局域网的核心，通过有线网络与 AP 相连，负责管理无线局域网中的 AP，集中管理控制 WLAN 中的无线 AP 设备。对 AP 的管理包括下发配置、修改相关配置参数、射频智能管理、接入安全控制，如图 8-1-9 所示。



图 8-1-9 无线控制器

传统的无线局域网中，没有集中管理的控制器设备，所有 AP 都通过交换机连接。每台 AP 单独负担射频、通信、身份验证、加密等工作，因此需要对每一台 AP 进行独立配置，难以实现全局、统一管理和集中的射频、接入和安全策略设置。

在基于无线控制器新型解决方案中，无线控制器能够出色地解决这些问题。在该方案中，所有 AP 都减肥（Fit AP），每台 AP 只负责射频和通信工作，类似于一个简单、基于硬件射频底层的传感设备。所有 Fit AP 接收到 RF 信号，经过 802.11 编码后，随即通过不同厂商制定加密隧道协议，穿过以太网并传送到无线控制器，进而由无线控制器集中对编码流进行加密、验证、安全控制等更高层次的工作。

如今的 Wi-Fi 网络覆盖，多采用 AC+AP 覆盖方式，无线局域网中有一台 AC（无线控制器），多台 AP（收发信号）。此模式应用于大中型企业中，有利于无线局域网的集中管理，多台无线发射器能统一发射一个信号（SSID），并且支持无缝漫游，以及 AP 射频的智能管理。

5. 天线

当无线工作站与无线 AP 或其他无线工作站相距较远时，随着信号的减弱，传输速率会明显下降，或者根本无法实现通信。此时，就必须借助于天线对所接收或发送的信号进行增益。无线天线有许多种类型，常见的有两种：一种是室内天线；另一种是室外天线。室外天线的类型比较多：一种是锅状的定向天线；另一种是棒状的全向天线，如图 8-1-10 所示。



图 8-1-10 天线产品

8.1.3 WLAN 的组网模式

组建无线网络时，可供选择的方案主要有两种：一种是无中心无线 AP 结构的 Ad-Hoc 网络模式；另一种为有中心无线 AP 结构的 Infrastructure（基础结构）网络模式。

这两种组网方式在无线网络规划中广泛应用，各有优缺点，各有不同应用场合。

1. Ad-Hoc 模式

Ad-Hoc 模式是点对点的对等结构，相当于有线网络中的两台计算机直接通过网卡互连，中间没有集中接入设备，信号是直接两个通信端点对点传输的，如图 8-1-11 所示。

在 WLAN 中，没有物理传输介质，而是以电磁波的形式发散传播的，所以在 WLAN 中的对等连接模式中，各用户无需安装多块 WLAN 网卡，相比有线网络来说，组网方式要简单许多。

Ad-Hoc 对等结构网络通信中没有一个信号交换设备，网络通信效率较低，所以仅适用于较少数量的无线结点互连（通常是在 5 台主机以内）。同时，由于这一模式没有中心管理单元，所以这种网络在可管理性和扩展性方面受到了一定的限制，连接性能也不是很好。而且各无线结点之间只能单点通信，不能实现交换连接，就像有线网络中的对等网一样。这种无线网络模式通常只适用于临时的无线应用环境，如小型会议室、SOHO 家庭无线网络等。

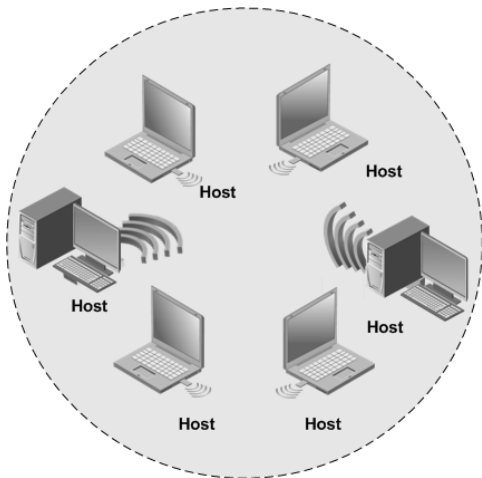


图 8-1-11 Ad-Hoc 模式无线局域网

2. Infrastructure 模式

Infrastructure 模式与有线网络中的星形交换模式相似，也属于集中式结构，其中无线 AP 相当于有线网络中的交换机或集线器，起着集中连接无线结点和数据交换的作用。通常无线 AP 都提供了一个有线以太网接口，用于与有线网络设备的连接，如以太网交换机。Infrastructure 模式的无线网络如图 8-1-12 所示。

Infrastructure 模式的特点主要表现在网络易于扩展、便于集中管理、能提供用户身份验证等方面，且其数据传输性能也明显高于 Ad-Hoc 模式。

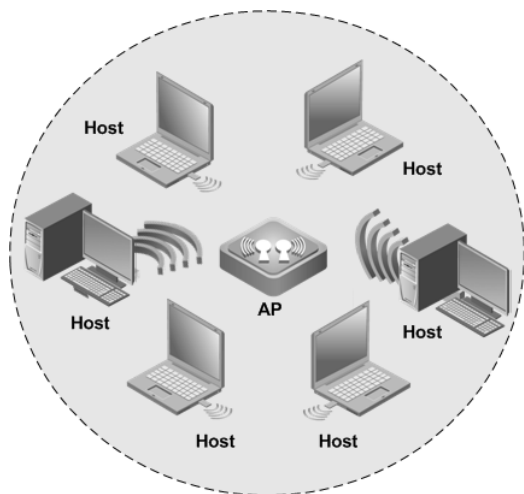


图 8-1-12 Infrastructure 模式的无线局域网

8.1.4 WLAN 的通信协议

由于无线网络也是局域网的一种分类，和有线局域网一样，IEEE 组织也为无线局域网的通信规划了一系列的通信标准。

到目前为止，IEEE 组织正式发布的无线网络协议主要包括 IEEE 802.11、IEEE 802.11a、IEEE 802.11b、IEEE 802.11g，分别对应于不同的传输标准。

1. IEEE 802.11

IEEE 802.11 是 IEEE 在 1997 年制定的第一个无线局域网标准，主要用于解决办公网和校园网中用户与用户终端的无线接入。业务主要限于数据存取，速率最高只能达到 2Mb/s。由于它在传输速率和传输距离上都不能满足人们的需要，因此 IEEE 又相继推出了 IEEE 802.11a 和 IEEE 802.11b 两个新标准。

2. IEEE 802.11b

IEEE 802.11b 标准是对 IEEE 802.11 的修正，IEEE 802.11b 标准传输速率提高到 11Mb/s，与普通的 10Base-T 有线网持平。802.11b 使用的是开放的 2.4GHz 频段，使用时无需申请，可直接作为有线网络的补充，又可独立组网，灵活性很强。

3. IEEE 802.11a

IEEE 802.11a 是 IEEE 802.11b 标准的修正，用于解决速度的问题，因此 IEEE 802.11a 使用 5.8GHz 频段传输信息，避开了微波、蓝牙及大量工业设备广泛采用的 2.4GHz 频段，在数据传输过程中，干扰大为降低，抗干扰性强，因此传输速率提高到 54Mb/s。

4. IEEE 802.11g

IEEE 802.11g 仍使用开放的 2.4GHz 频段，以保证和目前现有的很多设备的兼容性。但它

使用了改进的信号传输技术，在 2.4GHz 频段把速度提高到了 54Mb/s 的高速传输。

IEEE 802.11g 是目前被看好的无线网络标准，传输速率可以满足各种网络应用的需求。更重要的是，它还向下兼容 IEEE 802.11b 设备，但在抗干扰上仍不及 IEEE 802.11a。

5. IEEE 802.11n

802.11n 是在 802.11g 和 802.11a 之上发展起来的一项技术，最大的特点是速率提升，在传输速率方面，802.11n 可以将 WLAN 的传输速率由目前 802.11a 及 802.11g 提供的 54Mb/s，提高到 300Mbps，甚至高达 600Mb/s。

802.11n 可工作在 2.4GHz 和 5GHz 两个频段。

8.1.5 WLAN 的标识符 SSID

处于同一介质上互相连接的多台计算机通过广播帧的形式，把信息传播给网络中的所有设备，那么连接在无线网络环境中的所有设备又是如何来和自己的同伴进行通信的？又如何把无关的计算机排斥在无线网络范围之外呢？

实际上，处于同一网络中的无线设备为识别是否是自己的同伴，它们之间使用了一种无线网络身份标识符号来区别设备。就像对暗号一样，对得上暗号，就可以接入指定的网络，如果不知道这个暗号，就排斥在该无线网络之外，如图 8-1-13 所示。这种无线网络身份标识符号又称为 SSID。SSID 是配置在无线网络设备中一种无线标识，它允许具有相同 SSID 的无线用户端设备才能进行通信。因此 SSID 的泄密与否，也是保证无线网络接入设备安全的一个重要标志。

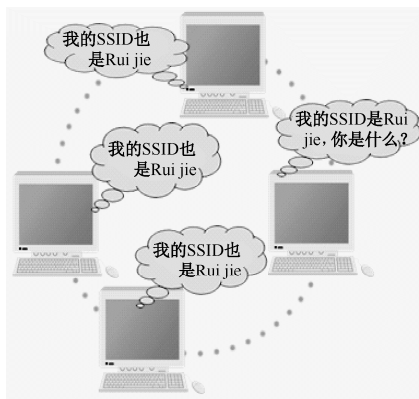


图 8-1-13 WLAN 的标识符 SSID

【综合实训】：组建 Ad-Hoc 模式无线局域网

网络场景

林东在房屋装修时，只预留了一个有线网络接口，现在家里中计算机增多了，需要重新



布置家庭网络，既不好走线，又影响居室美观。在考察朋友家中的无线网络环境后，林东希望在家中也规划一个全新的家庭无线网络。林东马上去计算机配件市场为家中所有的计算机分别购置了无线网卡，安装到计算机上开始组建一个简单的家庭无线网络，如图 8-1-14 所示。

实施过程

1. 打开配置窗口

在“网络连接”窗口中，选择“无线网络连接”图标，右击，选择快捷菜单中的“属性”命令，打开“无线网络连接 属性”对话框，选择“常规”选项卡中的“Internet 协议 (TCP/IP)”选项，单击“属性”按钮，如图 4-2-10 所示。

2. 配置无线局域网地址

在“Internet 协议 (TCP/IP) 属性”对话框中配置对等网络地址，IP 地址为 192.168.1.2，子网掩码为 255.255.255.0，如图 8-1-16 所示。



图 8-1-14 家庭无线网络



图 8-1-15 配置无线连接属性

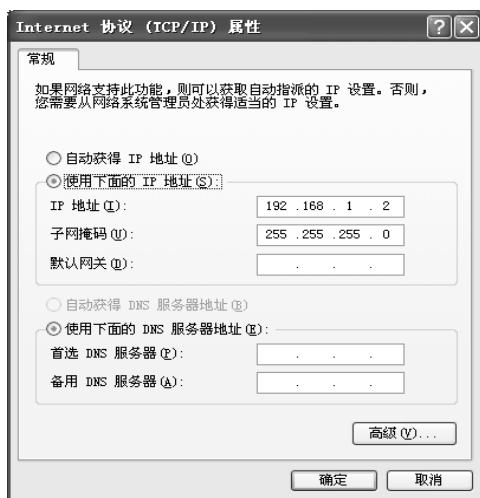


图 8-1-16 配置无线连接地址

3. 修改无线的标识

在“无线网络连接属性”对话框中选择“无线网络配置”选项卡，勾选“用 Windows 配置我的无线网络设置”复选框，使用 Windows 操作系统自带的软件包配置无线网络环境，如图 8-1-17 所示。

4. 添加一个新的标识

此时，“首选网络”选项组被激活，可以使用了。

单击“首选网络”选项组中的“添加”按钮，打开如图 8-1-18 所示的对话框，在“关

联”选项卡中将网络名（SSID）设置为 ruijie；网络验证为开放式；数据加密为已禁用。

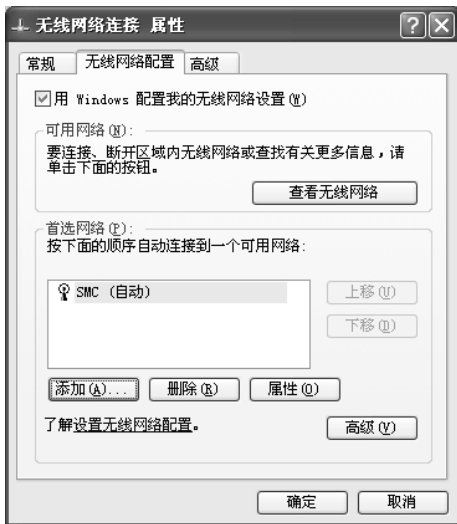


图 8-1-17 配置无线



图 8-1-18 配置无线网络属性

5. 添加一个新的标识

为无线网络中的设备添加标识名（SSID）为 ruijie，标识成功后的效果如图 8-1-19 所示。

6. 配置无线网络的连接模式

在“首选网络”选项组中选中标识名为 ruijie 的无线网络标识名，单击“高级”按钮。

打开“高级”对话框，选中“仅计算机到计算机（特定）”单选按钮，表示建设无线对等网络模式，如图 8-1-20 所示。



图 8-1-19 添加无线网络标识

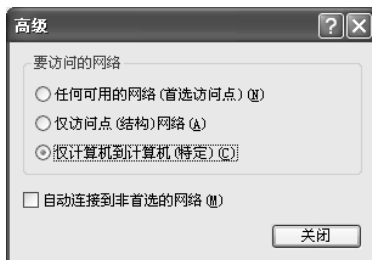


图 8-1-20 配置无线网络的连接模式

7. 查看状态

在“控制面板”中重新打开“网络连接”窗口，选择“无线网络连接”图标并双击，打开



“查看无线网络”对话框，其中将显示配置成功后的无线网络的连接状态，如图 8-1-21 所示。

8. 使用 Windows 连接无线网络

也可以在“网络连接”窗口中，选择“无线网络连接”图标并右击，选择快捷菜单中的“查看可用的无线连接”命令，使用 Windows 自带的“无线网络状态”小工具程序，如图 8-1-22 所示。



图 8-1-21 无线网络连接成功

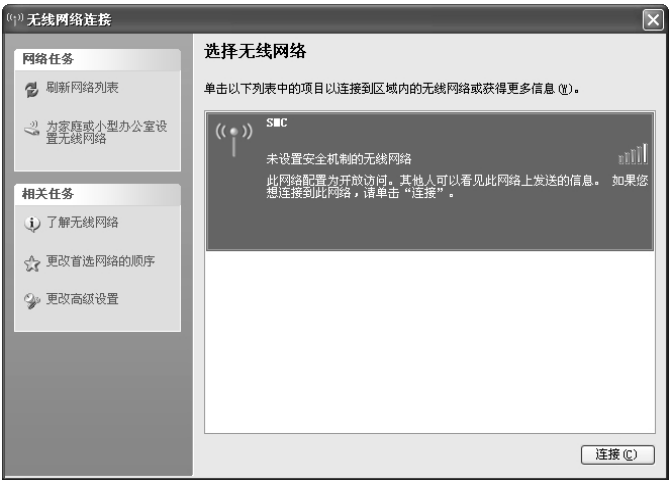


图 8-1-22 查看无线网络连接

9. 测试无线网络连通

打开无线网络中任意一台设备的“开始”菜单，选择“运行”命令，输入“cmd”后转到 DOS 命令行状态，如图 8-1-23 所示。



图 8-1-23 启动测试状态

10. 配置无线网卡地址

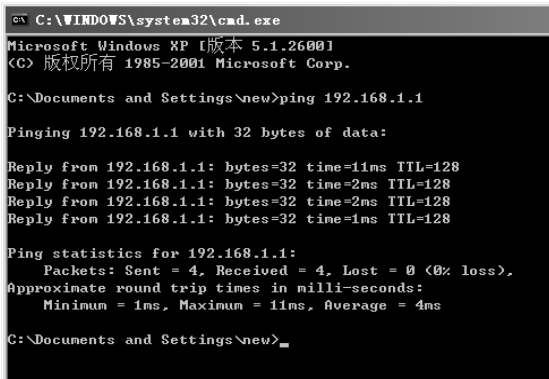
无线网卡 IP 地址配置信息如表 8-1-1 所示。

表 8-1-1 无线网卡 IP 地址配置信息

设备名	IP 地址	子网掩码
PC1	192.168.1.1	255.255.255.0
PC2	192.168.1.2	255.255.255.0

11. 测试连通性

使用 ping 命令，测试和另一台安装有无线网卡的 PC 的连通性，如图 8-1-24 所示。



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\new>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=11ms TTL=128
Reply from 192.168.1.1: bytes=32 time=2ms TTL=128
Reply from 192.168.1.1: bytes=32 time=2ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 4ms

C:\Documents and Settings\new>
```

图 8-1-24 测试网络连通性

任务 2 组建 Infrastructure 模式无线局域网

8.2.1 Infrastructure 无线网络基础

1. Infrastructure 模式

与 Ad-Hoc 结构无线网络模式不同，Infrastructure 结构的无线网络模式更加复杂，需要增加更多的无线互连设备。在 Infrastructure 结构中，无线网络计算机之间的通信通过无线接入设备进行连接，由 AP 转发信息，实现网络资源的共享。

2. Infrastructure 模式适用的场合

Ad-Hoc 结构的无线网络只适用于纯粹的无线环境或者数量有限的几台计算机之间的对接。在实际应用中，如果需要把无线网络和有线网络连接起来，或者有数量众多的计算机需要进行无线连接，则最好采用以无线 AP 为中心的 Infrastructure 模式。

Infrastructure 无线网络模式提供给用户更多的选择，既可以是纯粹的无线网络，又可以是无线和有线混合网络结构。

3. SSID

SSID 是无线网络中一个可配置的无线标识，它允许无线用户端与无线标识相同的无线 AP 之间进行通信。

通过配置无线网络中的设备，只有配有相同 SSID 的无线用户端设备才可以和无线 AP 通信。SSID 可以作为无线用户端和无线接入点之间传递的一个简单密码来看待，从而提供无线网络的安全保密功能。



8.2.2 胖 AP 基础知识

1. “胖” AP

AP 是 WLAN 网络中的重要组成部分，其工作机制类似于有线网络中的集线器，无线终端可以通过 AP 进行终端之间的数据传输，也可以通过 AP 的“WAN”口与有线网络互通，如图 8-2-1 所示。

通常，业界将 AP 分为“胖”AP 和“瘦”AP。

胖 AP 普遍应用于 SOHO 家庭网络或小型无线局域网，有线网络入户后，可以部署“胖”AP 进行室内覆盖，室内无线终端可以通过“胖”AP 访问。

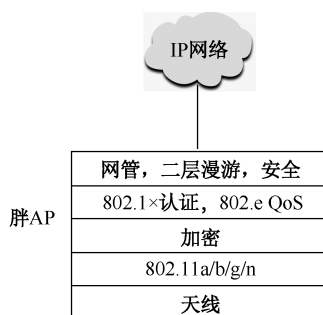


图 8-2-1 “胖” AP

2. 胖 AP 的特点

业界所谓的“胖”AP，其学名应该称之为无线路由器。无线路由器与纯 AP 不同，除无线接入功能外，一般具备 WAN、LAN 两个接口，多支持 DHCP 服务器、DNS 和 MAC 地址克隆，以及 VPN 接入、防火墙等安全功能。

通常，和瘦 AP 设备相比，胖 AP 具有如下特点。

- 需要每台 AP 单独进行配置，无法进行集中配置，管理和维护比较复杂。
- 支持二层漫游。
- 不支持信道自动调整和发射功率自动调整。
- 集安全、认证等功能于一体，支持能力较弱，扩展能力不强。
- 漫游切换的时候存在很大的时延。

胖 AP 设备仅限于 SOHO 或小型无线网络。在小规模的无线局域网部署时，胖 AP 是不错的选择。但是对于大规模无线部署，如大型企业网无线应用、行业无线应用及运营级无线网络，“胖”AP 无法支撑如此大规模的部署。

8.2.3 瘦 AP 基础知识

1. “瘦” AP

“瘦”AP 是指需要无线控制器进行管理、调试和控制的 AP。

“瘦”AP 设备的传输机制相当于有线网络中的集线器，在无线局域网中不停地接收和传送数据。每台无线 AP 基本上都拥有一个以太网接口，用于实现无线与有线的连接。任何一台装有无线网卡的 PC，均可通过 AP 来分享有线局域网络，甚至分享广域网络的资源。理论上，当网络中增加一台无线 AP 之后即可成倍地扩展网络覆盖直径，适合大规模搭建，可使网络中容纳更多的网络设备。

2. 无线控制器设备

对于企业用户来说，若要进行大面积的无线覆盖，没有无线 AP 是无法实现的。

由于每台 AP 平均能够支持的用户数只有 10~20 个，大型企业如果要部署无线网络，可能

需要几百台 AP 来使无线网络覆盖所有用户，这样就给无线局域网管理带来了很大麻烦。

2002 年第一个无线交换机诞生，这有效地改善了无线局域网的管理性能。无线交换机也称为无线控制器，是一种集中式的产品，它能够管理很多不具备智能的 AP。与“胖”AP 相比，“瘦”AP 的组网模式安装更简单、更且便宜，管理也非常容易。

无线控制器是一种无线局域网组网中应用到的网络设备，用来集中化控制无线瘦 AP 设备。无线控制器 AC 是无线网络的核心，负责管理无线网络中的所有无线瘦 AP 设备，对瘦 AP 设备的管理包括：下发配置、修改相关配置参数、射频智能管理、接入安全控制等。

8.2.4 无线控制器组网知识

无线控制器主要应用在大中型无线网络环境中，支持大数量 AP 环境场景，支持最多大数量的并发用户，支持 CAPWAP 协议，支持用户计费及认证功能，支持机内板卡 1+1，N+1 备份等运营级无线局域网工作环境，如图 8-2-2 所示。

在传统的无线网络中，没有集中管理的控制器设备，所有的 AP 都通过交换机连接起来，每台 AP 单独负担 RF、通信、身份验证、加密等工作，因此需要对每一台 AP 进行独立配置，难以实现全局的统一管理和集中的 RF、接入和安全策略设置。

而在基于无线控制器的新型解决方案中（AC + Fit AP），无线控制器能够出色地解决这些问题。在该方案中，每台 AP 只单独负责 RF 和通信的工作，其相当于一个简单的、基于硬件的 RF 底层传感设备。

所有 Fit AP 接收到的 RF 信号，经过 802.11 的编码之后，随即通过不同厂商制定的加密隧道协议穿过以太网络，并传送到无线控制器，进而由无线控制器集中对编码流进行加密、验证、安全控制等更高层次的工作。

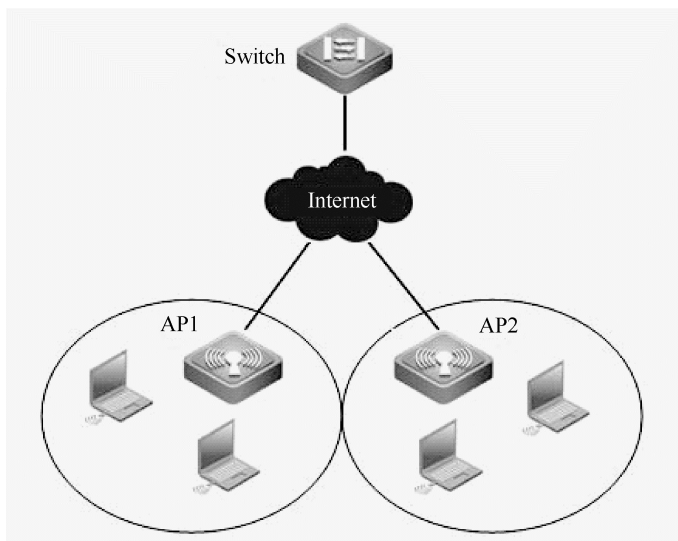


图 8-2-2 无线控制器组网

因此，基于 Fit AP 和无线控制器的无线网络解决方案，具有统一管理的特性，并能够出色地完成自动 RF 规划、接入和安全控制策略等工作。

传统无线与基于无线控制器方案的详细区别如表 8-2-1 所示。



表 8-2-1 传统无线与基于无线控制器方案的详细区别

评判标准	传统无线方案	基于无线控制器方案
技术模式	传统、主流	新生方式，增强型管理
安全性	传统加密、认证方式，普通安全性	增加射频环境监控，基于用户位置安全策略，高安全性
网络管理	对每个 AP 下发配置文件	无线交换机上配置好文件，AP 本身零配置
用户管理	类似有线，根据 AP 接入的有线端口区分权限	无线专门、虚拟专用组方式，根据用户名区分权限
WLAN 组网规模	二层漫游，适合小规模组网，成本较低	二层、三层漫游，拓扑无关性，适合大规模组网，成本较高
增值业务能力	仅实现简单数据接入	可扩展语音等丰富业务

【综合实训】：组建 Infrastructure 模式的无线局域网

网络场景

图 8-2-3 所示为某学校组建的无线校园网的工作场景，为保证学校礼堂的网络接入，安装了多台无线 AP 设备，通过 AP 设备覆盖整个礼堂的无线接入，使坐在礼堂各个角落的人都能通过无线信号接入校园网。同时，为了方便 AP 设备的统一管理，安装了无线交换机设备，统一管理全部的 AP，优化无线局域网的传输效率。

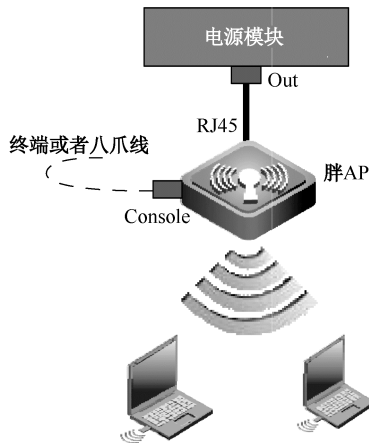


图 8-2-3 某学校礼堂的无线局域网络场景

实施过程

(1) 按照图 8-2-3 所示的网络拓扑，组建某学校礼堂的无线局域网。

(2) 配置“瘦”AP 设备：计算机通过配置线缆连接“瘦”AP 设备的控制端口，连接的方法同交换机设备连接。

在计算机上配置超级终端程序和 AP 设备连接的参数的方法也与配置交换机的方法相同。

备注：如果提示输入密码，则默认密码为 ruijie。

```
Password:ruijie (或 admin)
```

(3) 将 AP 切换为“胖”AP：AP 出厂设置默认为“瘦”AP，需要进行胖/瘦切换，如图 8-2-4 所示。

```
Ruijie>ap-mode fat
```

```
Ruijie>
Ruijie>ap?
ap-mode

Ruijie>ap
Ruijie>ap-mode ?
    fat  Fat mode
    fit  Fit mode

Ruijie>ap-mode fat
apmode will change to FAT.
Ruijie>
```

图 8-2-4 切换胖/瘦 AP

(4) AP 基本操作：关闭端口提示信息，如图 8-2-5 所示。

```
Ruijie>en
Ruijie#conf
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#no logging console
Ruijie(config)#
```

图 8-2-5 关闭端口提示信息

查看接口信息，如图 8-2-6 所示。

```
Ruijie(config)#show int gi0/1
Index(dec):1(hex):1
GigabitEthernet 0/1 is DOWN, line protocol is DOWN
Hardware is AHTEROS-SGMII GigabitEthernet, address is 1414.4b7a.514b (bia 1414.4b7a.514b)
Interface address is: 192.168.1.1/24
ARP type: ARPA, ARP Timeout: 3600 seconds
MTU 1500 bytes, BW 1000000 kbit
Encapsulation protocol is Ethernet-II, loopback not set
Keepalive interval is 10 sec, set
Carrier delay is 2 sec
RXload is 1, TXload is 1
Queueing strategy: FIFO
Output queue 0/40, 0 drops;
Input queue 0/75, 0 drops
Link Mode: Down, Media-Type is copper.
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer, 0 dropped
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
0 packets output, 0 bytes, 0 underruns, 0 dropped
...0 output errors, 0 collisions, 0 interface resets
```

图 8-2-6 查看接口信号

查看 AP 的工作模式，如图 8-2-7 所示。

```
Ruijie#show ap-mode
current mode: fat
Ruijie#
```

图 8-2-7 查看 AP 的工作模式

查看 AP 版本，如图 8-2-8 所示。

```
Ruijie#show version
System description      : Ruijie Indoor AP320-I (802.11a/n and 802.11b/g/n) By Ruijie Networks.
System start time       : 1970-01-01 0:0:0
System uptime           : 0:0:17:52
System hardware version : 1.10
System software version : RGOS 10.4(1b19)p2, Release(167368)
System boot version     : 10.4.137886(Master), 10.4.137886(Slave)
System serial number    : G1HD431043035
Ruijie#
```

图 8-2-8 查看 AP 版本



(5) 新建用户 VLAN 10，使用该 VLAN 通信。

注意：此 VLAN 只在本地有效，上送到交换机用户的数据不会带 VLAN 标签。

```
Ruijie(config)#vlan 10
Ruijie(config-vlan)#exit
```

(6) 上联以太网口封装 VLAN。

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#encapsulation dot1Q 10
```

(7) 定义 SSID。

```
Ruijie(config)#dot11 wlan 1          ! 创建 802.11 模式的 WLAN 的编号
Ruijie(dot11-wlan-config)#ssid ruijie
Ruijie(dot11-wlan-config)#broadcast-ssid
Ruijie(dot11-wlan-config)#vlan 10    ! 使 VLAN 10 和创建的 WLAN 1 关联
```

(8) 创建射频卡子接口（天线口为 802.11 的射频口）。

```
Ruijie(config)#interface dot11radio 1/0    ! 802.11 的射频口 1
Ruijie(config-subif)#encapsulation dot1Q 10
//封装 vlan 且此 vlan 和以太物理接口一致
Ruijie(config-subif)#mac-mode fat （默认）
```

备注：上面的命令用于配置第一根天线的关联；下面的命令用于配置第二根天线的关联。

```
Ruijie(config)#interface dot11radio 2/0    ! 802.11 的射频口 2
Ruijie(config-subif)#encapsulation dot1Q 10
Ruijie(config-subif)#mac-mode fat
```

(9) SSID 和射频卡进行关联。

```
Ruijie(config)#interface dot11radio 1/0    ! 进入射频物理口
Ruijie(config-if-Dot11radio 1/0)#wlan-id 1 ! 关联 WLAN 1
Config interface wlan id:1, SSID:ruijie    ! 提示映射成功
```

备注：上面的命令用于配置第一根天线的关联；下面的命令用于同样配置第二根天线的关联

```
Ruijie(config)#interface dot11radio 2/0
Ruijie(config-if-Dot11radio 2/0)#wlan-id 1
Config interface wlan id:1, SSID:ruijie    //提示映射成功
```

注意：步骤 (7)、步骤 (8)、步骤 (9) 的顺序不能颠倒，完成这一步之后可以看到 AP 已经发出无线信号。

(10) 配置 AP 的管理 IP 地址及默认路由。

```
Ruijie(config)#interface bvi 10    ! 配置桥虚拟接口 BVI
Ruijie(config-if-BVI 10)#ip add 172.16.1.253 255.255.255.0
Ruijie(config-if-BVI 10)#exit
Ruijie(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.1
! 给 AP 自己使用，为 AP 配置默认网关（可选，主要是远程关联）
```

(11) 手工配置 PC 的 IP 地址，测试无线局域网的连通性。